



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

1987

Cross-correlation of uniform cyclic difference set sequences.

Rogers, David L.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/22226>

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 96945-5002

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

CROSS-CORRELATION OF UNIFORM
CYCLIC DIFFERENCE SET SEQUENCES

by

David L. Rogers

June 1987

Thesis Advisor: Harold M. Fredricksen

Approved for public release; distribution is unlimited

T233646

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b RESTRICTIVE MARKINGS		
2a SECURITY CLASSIFICATION AUTHORITY			3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited		
2b DECLASSIFICATION/DOWNGRADING SCHEDULE			5 MONITORING ORGANIZATION REPORT NUMBER(S)		
4 PERFORMING ORGANIZATION REPORT NUMBER(S)			7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School		
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School		6b OFFICE SYMBOL (If applicable) Code 53	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000		
6c ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000			9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
8a NAME OF FUNDING/SPONSORING ORGANIZATION		8b OFFICE SYMBOL (If applicable)	10 SOURCE OF FUNDING NUMBERS		
8c ADDRESS (City, State, and ZIP Code)			PROGRAM ELEMENT NO	PROJECT NO	TASK NO
11 TITLE (Include Security Classification) CROSS-CORRELATION OF UNIFORM CYCLIC DIFFERENCE SET SEQUENCES					
12 PERSONAL AUTHOR(S) Rogers, David L.					
13a TYPE OF REPORT Master's Thesis		13b TIME COVERED FROM _____ TO _____		14 DATE OF REPORT (Year, Month, Day) 1987, June	
15 PAGE COUNT 96					
16 SUPPLEMENTARY NOTATION					
17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	Cross-Correlation; Cyclic Difference Sets; Maximal Length Linear Shift Register Sequences		
19 ABSTRACT (Continue on reverse if necessary and identify by block number)					
The incidence vector or characteristic function of a cyclic difference set can be viewed as a full period of a cyclic binary sequence. These cyclic difference set sequences possess certain desirable properties for applications in digital communications, radar ranging and some aspects of mathematical modeling. One particularly desirable property unique to cyclic difference set sequences is their two-level auto-correlation function. In this thesis, the cross-correlation functions of a sample of uniform cyclic difference set sequences are investigated. The cross-correlations involve equivalent and inequivalent uniform cyclic difference set sequences. In addition, the span and cyclotomic cosets are determined for each sequence in the sample.					
20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS			21 ABSTRACT SECURITY CLASSIFICATION Unclassified		
22a NAME OF RESPONSIBLE INDIVIDUAL Prof. Harold M. Fredricksen			22b TELEPHONE (Include Area Code) (408) 646-2206		22c OFFICE SYMBOL Code 53Fs

#18 - ABSTRACT (CONTINUED)

The number of values taken on by the cross-correlation function of two equivalent cyclic difference sets having a period of v is shown not to exceed the number of cyclotomic cosets modulo v . A conjecture is presented which states that the cross-correlation function of equivalent Hadamard quadratic residue sequences takes on three specified values. In partial support of the conjecture it is shown that the cross-correlation function of equivalent Hadamard quadratic residue sequences can not assume more than three values.

Approved for public release; distribution is unlimited

Cross-Correlation of Uniform
Cyclic Difference Set Sequences

by

David L. Rogers
Captain, United States Marine Corps
B.S., University of Alaska, Fairbanks, 1979

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
JUNE 1987

ABSTRACT

The incidence vector or characteristic function of a cyclic difference set can be viewed as a full period of a cyclic binary sequence. These cyclic difference set sequences possess certain desirable properties for applications in digital communications, radar ranging and some aspects of mathematical modeling. One particularly desirable property unique to cyclic difference set sequences is their two-level auto-correlation function.

In this thesis, the cross-correlation functions of a sample of uniform cyclic difference set sequences are investigated. The cross-correlations involve equivalent and inequivalent uniform cyclic difference set sequences. In addition, the span and cyclotomic cosets are determined for each sequence in the sample.

The number of values taken on by the cross-correlation function of two equivalent cyclic difference sets having a period of v is shown not to exceed the number of cyclotomic cosets modulo v . A conjecture is presented which states that the cross-correlation function of equivalent Hadamard quadratic residue sequences takes on three specified values. In partial support of the conjecture it is shown that the cross-correlation function of equivalent Hadamard quadratic residue sequences can not assume more than three values.

TABLE OF CONTENTS

I.	INTRODUCTION -----	9
II.	CYCLIC DIFFERENCE SETS -----	11
	A. DEFINITION AND EXAMPLES -----	11
	B. EQUIVALENCE AND COMPLEMENTS -----	12
	C. MULTIPLIERS AND CYCLOTOMIC COSETS -----	13
	D. INCIDENCE VECTORS AND AUTOCORRELATION -----	15
	E. SPECIAL TYPES OF CYCLIC DIFFERENCE SETS -----	18
	F. CYCLIC DIFFERENCE SET SEQUENCES -----	24
III.	MAXIMAL LENGTH LINEAR SHIFT REGISTER SEQUENCES ---	27
	A. LINEAR SHIFT REGISTER SEQUENCES -----	27
	B. PSEUDO-RANDOMNESS PROPERTIES -----	30
	C. M-SEQUENCE MULTIPLIERS AND CYCLOTOMIC COSETS -	31
	D. DECIMATION -----	32
	E. TRACE -----	35
	F. SHIFT AND ADD PROPERTY -----	40
	G. REGULARITIES IN CROSS-CORRELATION -----	44
IV.	METHODOLOGY -----	50
	A. PROCEDURE -----	50
	B. CYCLOTOMIC COSETS AND EQUIVALENT SEQUENCES ---	53
	C. CROSS-CORRELATION -----	55
V.	RESULTS -----	61
	A. REMARKS -----	61
	B. CROSS-CORRELATION OF INEQUIVALENT SEQUENCES --	61

C.	CROSS-CORRELATION OF EQUIVALENT SEQUENCES ----	62
D.	CROSS-CORRELATION OF EQUIVALENT QUADRATIC RESIDUE SEQUENCES -----	64
VI.	CONCLUSIONS -----	72
APPENDIX A:	SAMPLE CYCLIC DIFFERENCE SETS -----	74
APPENDIX B:	CYCLOTOMIC COSETS -----	78
APPENDIX C:	INEQUIVALENT CROSS-CORRELATIONS -----	85
APPENDIX D:	EQUIVALENT CROSS-CORRELATIONS -----	87
LIST OF REFERENCES	-----	94
INITIAL DISTRIBUTION LIST	-----	95

LIST OF TABLES

III.1	NON-ZERO ELEMENTS OF $E = GF(2^4)$ -----	38
IV.1	SAMPLE CYCLIC DIFFERENCE SETS -----	52
IV.2	PERIOD DISTRIBUTION OF INEQUIVALENT SEQUENCES --	57

LIST OF FIGURES

III.1	General Shift Register with Feedback -----	27
-------	--	----

I. INTRODUCTION

To every cyclic (v, k, λ) -difference set D there corresponds a binary sequence, $\{s_i\}$ $i = 0, 1, 2, \dots, v-1$, determined by its incidence vector or characteristic function. The characteristic function places a 1 in position i of the v -long sequence if i is an element of the cyclic difference set and places a 0 in position i otherwise. The sequence $\{s_i\}$ can be extended bi-infinitely to form a periodic sequence of period v . We call the binary sequences which have the same period v , uniform sequences of period v . Certain cyclic difference set sequences possess the pseudo-randomness properties generally described as balance, run and two-level auto-correlation. These properties make the cyclic difference set sequences desirable for applications in digital communications, radar ranging, and some aspects of mathematical modeling. One property common to all cyclic difference set sequences is their two-level auto-correlation function. However, not all of these sequences are balanced or have the run property.

The maximal length linear shift register sequences (M-sequences) are examples of cyclic difference set sequences which have been studied extensively. In the following sections we observe regularities in the cross-correlation function of uniform M-sequences. In particular,

the number of values assumed by the cross-correlation of uniform M-sequences of period v never exceeds $Y(v)$, the number of cyclotomic cosets, modulo v . When the correlation is between an M-sequence and a cyclically shifted version of the same sequence (auto-correlation) then the number of values taken on is two. The cross-correlation function of two cyclically distinct, uniform M-sequences assumes only three values on occasion but never less than three values.

This thesis investigates the cross-correlation functions for a sample of uniform cyclic difference set sequences. The cross-correlations are presented along with other distinguishing properties of the cyclic difference set sequences. These properties include the multipliers, span and cyclotomic cosets.

II. CYCLIC DIFFERENCE SETS

A. DEFINITION AND EXAMPLES

A set $D = \{r_1, r_2, \dots, r_k\}$ of k distinct residues modulo v is called a cyclic (v, k, λ) -difference set if for every residue $\alpha \not\equiv 0 \pmod{v}$ there are exactly λ ordered pairs (r_i, r_j) from D such that $r_i - r_j \equiv \alpha \pmod{v}$. This definition immediately imposes the following relation

$$k(k-1) = (v-1)\lambda \quad (1.1)$$

which must necessarily hold among the three parameters v , k and λ . This can be seen by observing that there are $k(k-1)$ distinct ordered pairs from D and $(v-1)$ nonzero residues $\pmod{v}$ which must each occur λ times.

The following trivial cyclic difference sets exist for every positive integer v :

$D = \emptyset$	$(v, k, \lambda) = (v, 0, 0)$
$D = \{i\}, 0 \leq i \leq v-1$	$(v, k, \lambda) = (v, 1, 0)$
$D = \{0, 1, 2, \dots, v-1\}$	$(v, k, \lambda) = (v, v, v)$
$D = \{0, 1, 2, \dots, i-1, i+1, \dots, v-1\}$	$(v, k, \lambda) = (v, v-1, v-2).$

These trivial cases are generally ignored or only treated as limiting cases. If the additional parameter $n = k - \lambda$ is

considered it can be shown by equation 1.1 that these trivial cases occur iff $n = 0$ or $n = 1$. A few examples of non-trivial cyclic difference sets are:

$$\begin{array}{ll} D = \{1,3,4,5,9\} & (v,k,\lambda) = (11,5,2) \\ D = \{0,2,6,7,8,10\} & (v,k,\lambda) = (11,6,3) \\ D = \{0,1,2,4,5,8,10\} & (v,k,\lambda) = (15,7,3). \end{array}$$

B. EQUIVALENCE AND COMPLEMENTS

Let z be any integer and $D = \{r_1, r_2, \dots, r_k\}$ be a cyclic (v, k, λ) -difference set. If the set D^* is formed by adding z , modulo v , to every element of D as follows

$$D^* = \{r_1+z, r_2+z, \dots, r_k+z\} = D+z \pmod{v}$$

then it should be apparent that D^* is also a cyclic (v, k, λ) -difference set. D^* is said to be a cyclic shift of D . If q is an integer, relatively prime to v , then the set D^{**} formed by multiplying every element of D by q , modulo v , as follows

$$D^{**} = \{qr_1, qr_2, \dots, qr_k\} = qD \pmod{v}$$

is also a cyclic (v, k, λ) -difference set. Any two cyclic (v, k, λ) -difference sets, D_k and D_j , are said to be

equivalent if $D_k = qD_j + z$, modulo v , for some integers q and z with q relatively prime to v [Ref. 1:pp. 1-2].

If D is a cyclic (v, k, λ) -difference set then its complement $\bar{D} = \{0, 1, \dots, v-1\} \setminus D$ is a cyclic $(v, v-k, v-2k+\lambda)$ -difference set [Ref. 1: pp. 2-3]. It is usually sufficient to consider only one of a pair of complementary cyclic difference sets. This can be accomplished by requiring that k be strictly less than $v/2$. Equation 1.1 precludes the possibility that k is equal to $v/2$. Note, if $k = v/2$ then $v = 2\lambda \pm \sqrt{(2\lambda)^2 + 1}$ by equation 1.1. Hence, if $\lambda = 0$ then $v = \pm 1$ and $k = \pm 1/2$ which is a contradiction. Alternatively, if λ is a positive integer then $\sqrt{(2\lambda)^2 + 1}$ is clearly irrational and the contradiction that v is irrational immediately follows.

C. MULTIPLIERS AND CYCLOTOMIC COSETS

If, for a given cyclic (v, k, λ) -difference set D and an integer m relatively prime to v , there exists an integer s such that $mD \equiv D + s$, modulo v , then m is called a multiplier of the cyclic difference set D . The multipliers of D collectively form a multiplicative group, modulo v [Ref. 2: pp. 131-132].

Multipliers play a large role in the construction of certain cyclic difference sets and in proving the nonexistence of other particular types. All known cyclic difference sets have non-trivial multipliers and it remains an open question as to whether this must hold for all cyclic

difference sets [Ref. 1:pp. 7-8]. The following theorem, the "multiplier theorem", provides for the existence of multipliers for cyclic difference sets in certain cases.

Theorem II.1

If $D = \{r_1, r_2, \dots, r_k\}$ is a cyclic (v, k, λ) -difference set and if p is a prime divisor of $n = k - \lambda$ such that $(p, v) = 1$ and $p > \lambda$, then p is a multiplier of the cyclic difference set D .

A proof of Theorem II.1 is provided by Hall and is beyond the scope of this presentation [Ref. 2:pp. 132-135].

The multiplier m of a cyclic difference set can be characterized as inducing an automorphism, $r \rightarrow rm \pmod{v}$ of the underlying abelian group. This automorphism is thus a permutation of the integers $\{0, 1, 2, \dots, v-1\}$ and can be expressed in cycle form [Ref. 3:pp. 90-91]. The cycles of the permutation $r \rightarrow rm \pmod{v}$ are called cyclotomic cosets. As an example, consider the case $v = 15$ and $m = 2$ with the corresponding permutation Π_m .

$$\Pi_m = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 \end{bmatrix}$$

This permutation of the residues, modulo 15, can be expressed in cycle form as

(0), (1,2,4,8), (3,6,12,9), (5,10), (7,14,13,11)

and the corresponding sequentially indexed cyclotomic cosets are listed as follows:

$$C_0 = \{0\}$$

$$C_1 = \{1,2,4,8\}$$

$$C_2 = \{3,6,12,9\}$$

$$C_3 = \{5,10\}$$

$$C_4 = \{7,14,13,11\}.$$

D. INCIDENCE VECTORS AND AUTOCORRELATION

Associated with every cyclic (v,k,λ) -difference set D is the binary sequence $\{s_i\}$ $i = 0,1,2,\dots,v-1$, which can be considered as bi-infinite and periodic with a period of v . The sequence is produced by the incidence vector or characteristic function of the cyclic difference set

$$s_i = \begin{cases} 1 & \text{if } i \in D \\ 0 & \text{otherwise.} \end{cases}$$

For example, the binary sequence given as

0 1 0 1 1 1 0 0 0 1 0

of length 11 is associated with the cyclic (11,5,2)-difference set $D = \{1,3,4,5,9\}$. This sequence can be extended bi-infinitely

...0 1 0 1 1 1 0 0 0 1 0 0 1 0 1 1 1 0 0 0 1 0...

to form the periodic cyclic difference set sequence of period 11.

The set of periodic binary sequences can be partitioned into distinct classes. Each class is composed of all the periodic binary sequences which have the same period. Any collection of sequences which are in the same class are called uniform.

The autocorrelation function of a sequence $\{s_i\}$ having a period of v is given as

$$C_S(\tau) = \sum_{i=0}^{n-1} s_i s_{i+\tau}$$

where the subscripts are taken, modulo v . Since $\{s_i\}$ is the characteristic function of a cyclic difference set its autocorrelation function is evaluated as: [Ref. 1:p. 6]

$$C_S(\tau) = \begin{cases} k & \text{if } \tau \equiv 0 \pmod{v} \\ \lambda & \text{otherwise.} \end{cases}$$

The binary sequence $\{s_i\}$ can be transformed to the equivalent sequence $\{x_i\}$ by

$$x_i = 1 - 2s_i$$

which merely replaces the ones of $\{s_i\}$ with negative ones and the zeros of $\{s_i\}$ with ones. If the sequence $\{x_i\}$ is correlated against its cyclic shifts $\{x_{i+\tau}\}$, where $\tau \neq 0$, modulo v , the value $(-1 \cdot -1)$ is obtained exactly λ times, $(-1 \cdot 1)$ and $(1 \cdot -1)$ are each obtained $k - \lambda$ times and $(1 \cdot 1)$ is obtained the remaining $v - 2(k - \lambda) - \lambda$ times [Ref. 4:p. 59]. The following example illustrates this evaluation:

$$\begin{aligned} D &= \{1, 2, 4\} & (v, k, \lambda) &= (7, 3, 1) \\ \{x_i\} &= 1 \ -1 \ -1 \ 1 \ -1 \ 1 \ 1 \\ \{x_{i+1}\} &= -1 \ -1 \ 1 \ -1 \ 1 \ 1 \ 1 \\ \{x_{i+2}\} &= -1 \ 1 \ -1 \ 1 \ 1 \ 1 \ -1 \\ \{x_{i+3}\} &= 1 \ -1 \ 1 \ 1 \ 1 \ -1 \ -1 \\ \{x_{i+4}\} &= -1 \ 1 \ 1 \ 1 \ -1 \ -1 \ 1 \\ \{x_{i+5}\} &= 1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1 \\ \{x_{i+6}\} &= 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1. \end{aligned}$$

Correlating $\{x_i\}$ against $\{x_{i+3}\}$, we obtain the value $(-1 \cdot -1)$ exactly once, $(-1 \cdot 1)$ and $(1 \cdot -1)$ two times each and $(1 \cdot 1)$ the remaining two times. If $\{x_i\}$ is correlated against itself, the value $(-1 \cdot -1)$ is obtained exactly k times and $(1 \cdot 1)$ is

obtained the remaining $v-k$ times. The autocorrelation function of $\{x_i\}$ is given as

$$C_Y(\tau) = \begin{cases} v & \text{if } \tau \equiv 0 \pmod{v} \\ v-4(k-\lambda) & \text{otherwise.} \end{cases}$$

This type of autocorrelation function is said to be two-level. The cyclic difference set sequences are the only binary sequences which possess two-level autocorrelation functions [Ref. 1:p. 7].

E. SPECIAL TYPES OF CYCLIC DIFFERENCE SETS

The cyclic (v, k, λ) -difference sets are generally classified by some relationship that exists among the parameters v , k , λ and n . The parameters v and n are generally viewed as the most fundamental of the four. Given a cyclic (v, k, λ) -difference set D and its complement $\bar{D}$ with parameters $(\bar{v}, \bar{k}, \bar{\lambda}) = (v, v-k, v-2k+\lambda)$, it follows from equation (1.1) that

$$\overline{k \cdot k} = k(v-k) = n(v-1)$$

$$\lambda \cdot \bar{\lambda} = (v-2k+\lambda) = n(n-1).$$

Noting that $\lambda + \bar{\lambda} = v-2n$ and requiring $\lambda \geq 1$ for non-trivial cyclic difference sets, it then follows that

$$(v-2n)^2/4 \geq \lambda \cdot \bar{\lambda} = n(n-1) \geq v-2n-1$$

hence,

$$n^2+n+1 \geq v \geq 4n-1. \quad (2.1)$$

The parameters of all cyclic (v, k, λ) -difference sets are constrained by equation 2.1. [Ref. 1:p. 3].

Certain types of cyclic (v, k, λ) -difference sets have been investigated to a greater extent than others. These types or classes are characterized by special relationships that exist among the parameters v , k , λ and n in addition to equation (2.1). For example, the Hadamard cyclic difference sets have parameters $v = 4t-1$, $k = 2t-1$, and $\lambda = t-1$ for some positive integer t . Cyclic difference sets are also categorized into families if the common property among them is of a constructive nature. These categories serve to identify and distinguish inequivalent cyclic difference sets which have identical parameters of v , k and λ . The following three sections describe some of the categories that are more commonly encountered.

1. Planar Type

The cyclic difference sets that correspond to finite cyclic projective planes with $\lambda = 1$ are described as being planar or simple. An extensive treatment of finite projective geometries can be found in Lidl and Neiderreiter

[Ref. 5:pp. 496-508] and Coxeter [Ref. 6:pp. 229-262]. Planar cyclic difference sets are known to exist with parameters $v = p^{2j} + p^{j+1}$, $k = p^{j+1}$ and $\lambda = 1$ for all prime powers $p^j = n$. Note, p^k is a multiplier of such cyclic difference sets for all positive integers k by the Multiplier Theorem II.1. All known planar cyclic difference sets are in the Singer family which are related to finite projective geometries, and have parameters

$$v = (q^{(N+1)} - 1)/(q - 1), \quad k = (q^N - 1)/(q - 1), \quad \lambda = (q^{(N-1)} - 1)/(q - 1)$$

where $N \geq 1$ and q is a prime power [Ref. 1:pp. 77-78,99]. Since $n = k - \lambda = (q^N - q^{(N-1)})/(q - 1)$, q^{N-1} is a multiplier of all such cyclic difference sets. A few examples of planar cyclic difference sets are provided as follows:

$D_1 = \{1, 2, 4\}$	$(v, k, \lambda) = (7, 3, 1)$
$D_2 = \{0, 1, 3, 9\}$	$(v, k, \lambda) = (13, 4, 1)$
$D_3 = \{3, 6, 7, 12, 14\}$	$(v, k, \lambda) = (21, 5, 1)$
$D_4 = \{1, 5, 11, 24, 25, 27\}$	$(v, k, \lambda) = (31, 6, 1)$

with multipliers 2^{t_1} , 3^{t_2} , 2^{t_3} and 5^{t_4} for positive integers t_1 , t_2 , t_3 and t_4 , respectively.

2. Hadamard Type

The Hadamard cyclic difference sets are characterized by possessing parameters (v, k, λ) of the form

$v = 4t-1$, $k = 2t-1$ and $\lambda = t-1$. The Hadamard cyclic difference sets share a common characteristic with the planar cyclic difference sets in that they both possess the extreme values of λ [Ref. 1:pp. 90-91]. This is seen by requiring $k < v/2$ as usual, so that $1 \leq \lambda \leq (v-3)/4$. All known Hadamard cyclic difference sets can be categorized according to the value of v as follows:

- (i) $v = 2^j - 1$, $j \geq 2$
- (ii) $v = 4t-1$, v is prime
- (iii) $v = 4t-1 = 4x^2+27$, v is prime
- (iv) $v = p(p+2)$, p and $p+2$ are both prime.

Since $n = t > \lambda = t-1$, t^k is a multiplier whenever t is prime.

The cyclic difference sets in category (i) are included in the Singer family which means that there exists an explicit method for their construction [Ref. 1:pp. 99-119]. Those in category (ii) include the quadratic residues, modulo v , among others. The cyclic difference sets in category (iii) are called Hall cyclic difference sets and those in category (iv) are called the twin prime cyclic difference sets.

It does happen that inequivalent Hadamard type cyclic difference sets with identical parameters v , k and λ belong to more than one category. This, of course, implies

an overlap of the categories exists. In particular, the following overlaps are listed [Ref. 1:pp. 90-91]:

- (a) (i) and (ii) overlap iff v is a Mersenne prime
- (b) (i) and (iii) overlap iff $v = 31$ or 127 or 131071
- (c) (i) and (iv) overlap iff $v = 15$.

Some Hadamard type cyclic difference sets are given in the following examples:

$$D_1 = \{1, 2, 4\}$$

$$(v, k, \lambda) = (7, 3, 1); \text{ categories (i) \& (iii)}$$

$$D_2 = \{1, 3, 4, 5, 9\}$$

$$(v, k, \lambda) = (11, 5, 2); \text{ category (ii)}$$

$$D_3 = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}$$

$$(v, k, \lambda) = (31, 15, 7); \text{ categories (i) \& (iii)}$$

$$D_4 = \{0, 1, 2, 4, 5, 8, 10\}$$

$$(v, k, \lambda) = (15, 7, 3); \text{ category (iv)}.$$

3. N^{th} Power Residue Type

A cyclic (v, k, λ) -difference set whose elements are the N^{th} powers, modulo v , where v is a prime is called an N^{th} power residue cyclic difference set. If zero is added

to this set the resulting set is called a modified N^{th} power residue cyclic difference set. The quadratic residue cyclic difference sets are a well known class of N^{th} power cyclic difference sets which are also of the Hadamard type. Theorem II.2 describes the existence of quadratic residue cyclic difference sets of the Hadamard type when $v = 4t-1$ for some positive integer t .

Theorem II.2

If $v = 4t-1$ is a prime, the quadratic residues, modulo v , form a cyclic difference set with parameters

$$(v, k, \lambda) = (4t-1, 2t-1, t-1).$$

Baumert [Ref. 1:p. 119] provides a complete proof of this theorem.

Recall that an integer $\alpha \not\equiv 0$, modulo p , where p is an odd prime, is called a quadratic residue, modulo p , if the congruence $x^2 \equiv \alpha \pmod{p}$ has a solution $x \pmod{p}$. Otherwise, α is called a quadratic non-residue, modulo p . An example of a quadratic residue cyclic difference set is

$$D = \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \qquad (v, k, \lambda) = (19, 9, 4).$$

The congruences $x^2 \pmod{19}$ are:

$$\begin{array}{llllll}
1^2 \equiv 1, & 18^2 \equiv 1, & 4^2 \equiv 16, & 15^2 \equiv 16, & 7^2 \equiv 11, & 12^2 \equiv 11 \\
2^2 \equiv 4, & 17^2 \equiv 4, & 5^2 \equiv 6, & 14^2 \equiv 6, & 8^2 \equiv 7, & 11^2 \equiv 7 \\
3^2 \equiv 9, & 16^2 \equiv 9, & 6^2 \equiv 17, & 13^2 \equiv 17, & 9^2 \equiv 5, & 10^2 \equiv 5.
\end{array}$$

Clearly, if $x^2 \equiv \alpha \pmod{p}$ then $(p-x)^2 \equiv \alpha \pmod{p}$ since

$$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}.$$

Therefore, the congruences $x^2 \pmod{p}$ need only be determined for the residues $x = 1, 2, \dots, (p-1)/2$.

The following theorem identifies the multipliers for all N^{th} power cyclic difference sets.

Theorem II.3

The N^{th} power residues themselves are the only multipliers of a non-trivial N^{th} power residue cyclic difference set.

A proof of Theorem II.3 is given by Baumert [Ref. 1:pp. 125-126].

A full treatment on the classification and construction of cyclic difference sets can be found in Baumert [Ref. 1] and Hall [Ref. 2:pp. 120-166].

F. CYCLIC DIFFERENCE SET SEQUENCES

The discussion so far has focused primarily on cyclic difference sets. In Section II.D it was shown that a binary

sequence can be associated with each cyclic difference set by means of its incidence vector or characteristic function. These cyclic difference set sequences are the only binary sequences which possess a two-level auto-correlation function. The two-level auto-correlation function makes them useful for applications in digital communications and radar ranging.

The remainder of this thesis deals specifically with cyclic difference set sequences which are extended periodically. The period of each cyclic difference set sequence is, of course, v . These sequences are identified by their associated cyclic differences sets. The general properties of all cyclic difference sets such as their multipliers, shifts and cyclotomic cosets carry over in a natural way to their associated cyclic sequences.

A cyclic difference set D can be transformed to an equivalent cyclic difference set D^* by forming the product dD , modulo v , where d is a multiplier of D . In a similar fashion, the periodic binary sequence $\{s_i\}$ associated with D can be transformed to an equivalent cyclically shifted version $\{s_{di}\}$ by taking every d^{th} element, modulo v , from $\{s_i\}$. This process is called decimation. Hence, if $\{s_i\}$ is decimated by any element d from its associated multiplier group, then $\{s_{di}\} = \{s_{i+\tau}\}$ for some integer τ . There exists a particular shift of $\{s_i\}$ for which a decimation by any of its multipliers results in an identical sequence so that

$\{s_{di}\} = \{s_i\}$. In this case $\{s_i\}$ is said to be in its characteristic shift.

The cyclotomic cosets of a cyclic difference set sequence are determined by its associated multiplier group G . These cosets are constructed by forming the products $rg \pmod v$ where r is an arbitrary residue, modulo v . The cyclotomic cosets are intimately connected with the structure of their corresponding cyclic difference set sequences. For instance, if the cyclic difference set sequence $\{s_i\}$ is in its characteristic shift, then the values observed in all the positions of the sequence which lie in any particular cyclotomic coset of $\{s_i\}$ will be identical. This property of cyclic difference set sequences is described as being "constant on cosets" for obvious reasons.

The "constant on cosets" property can be exploited to construct cyclic difference sets and their associated sequences. For a given modulus v , the cyclotomic cosets of each non-trivial multiplier d can be constructed, then all possible combinations of the cosets are selected and their elements are combined into a set of cardinality k . This set is then tested to determine if the requirements for a cyclic (v, k, λ) -difference set are met, i.e. if each non-zero difference α occurs exactly λ times.

III. MAXIMAL LENGTH LINEAR SHIFT REGISTER SEQUENCES

A. LINEAR SHIFT REGISTER SEQUENCES

The cyclic difference set sequences include a special type of periodic binary sequences known as maximal length linear shift register sequences (M-sequences). A general (nonlinear) shift register of span n is an electronic device consisting of n sequentially connected binary storage units. At regular intervals the contents of each unit is shifted down the line into the next storage unit. During this shift a feedback term is computed from the contents of the n units and fed back into the first storage unit. The feedback term is determined by a feedback function which, in general, is not a linear combination of the values in the n storage units. Figure III.1 shows the general block diagram of a general (nonlinear) shift register with feedback.

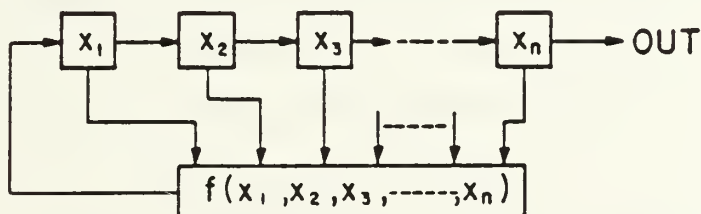


Figure III.1 General Shift Register with Feedback.

The behavior of the shift register can be described as a mapping from a binary n -tuple space to itself which is invoked at regular intervals. The mapping is depicted as

$$(x_1, x_2, \dots, x_n) \rightarrow (f(x_1, \dots, x_n), x_1, x_2, \dots, x_{n-1}).$$

The actual output of the shift register can be taken as the binary sequence generated from the history of any particular storage unit or as the sequential progression of the binary n -tuples themselves.

A linear shift register of span n generates a sequence of elements $\{s_i\}$ from the finite field $F = GF(2)$. The elements of $\{s_i\}$ satisfy an n^{th} order linear recurrence relation over F of the form

$$s_t = a_1 s_{t-1} + a_2 s_{t-2} + \dots + a_n s_{t-n} \quad (3.1)$$

where the coefficients $a_1, a_2, \dots, a_n$ are fixed elements of F and $a_n \neq 0$. The characteristic polynomial of the linear recurrence relation defined by equation (3.1) is defined as

$$c(x) = x^n - a_1 x^{n-1} - a_2 x^{n-2} - \dots - a_n.$$

The elements of an M -sequence satisfy an n^{th} order linear recurrence relation over $F = GF(2)$ whose characteristic polynomial $c(x)$ is primitive, i.e. $c(x)$ is an

n^{th} degree irreducible polynomial over $F = GF(2)$ which is the minimal polynomial of a primitive root α in $E = GF(2^n)$. This means that α generates the multiplicative group of non-zero elements in $E = GF(2^n)$ and that $c(x)$ is the unique monic irreducible n^{th} degree polynomial in $F[x]$ for which $c(\alpha) = 0$. For example, one period of an M-sequence having a period of $v = 7$ is

$$\{s_k\} = 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0.$$

The elements of this M-sequence satisfy the 3rd order linear recurrence relation

$$s_t = s_{t-1} + s_{t-3}$$

which has the characteristic polynomial

$$c(x) = x^3 - x^2 - 1$$

The shift register configured as in Figure III.1 that generates $\{s_k\}$ has corresponding feedback function

$$f(x_1, x_2, x_3) = x_1 + x_3.$$

where the sum of x_1 and x_3 is reduced modulo 2.

B. PSEUDO-RANDOMNESS PROPERTIES

Every M-sequence of period $v = 2^n - 1$ satisfies three basic pseudo-randomness properties [Ref. 4:p. 10]. These properties make it appear that the elements of an M-sequence are determined entirely by a random process. However, M-sequences are deterministic and not random. Therefore, the three properties are said to be pseudo-random. They are listed as follows:

- (i) Balance Property. There are 2^{n-1} ones and $2^{n-1}-1$ zeros in every period.
- (ii) Run Property. There are 2^{n-2-i} runs of ones and 2^{n-2-i} runs of zeros of length i , for $1 \leq i \leq n-2$, plus a single run of $n-1$ zeros and a single run of n ones in each period.
- (iii) Correlation Property. The autocorrelation function takes on the value $v = 2^n - 1$ if $j \equiv 0 \pmod{v}$ and -1 otherwise.

Note that the correlation property essentially states that M-sequences have a two-level autocorrelation function. Hence, every M-sequence represents the incidence vector of a cyclic difference set. It can be shown that this cyclic difference set has parameters $(v, k, \lambda) = (2^n - 1, 2^{n-1}, 2^{n-2})$

[Ref. 7:p. 730]. M-sequences also have the additional property that all 2^{n-1} subsequences of length n in the sequence are distinct [Ref. 3:pp. 152-153].

C. M-SEQUENCE MULTIPLIERS AND CYCLOTOMIC COSETS

Since it has been determined that an M-sequence represents the incidence vector of a cyclic difference set, the question of identifying its associated multipliers naturally arises. The following theorem identifies the multipliers of all M-sequences.

Theorem III.1

If $\{s_k\}$ is a maximal length linear shift register sequence of degree n , then $\{s_{qk}\}$ is equivalent to a cyclically shifted version of $\{s_k\}$ iff

$$q = 1, 2, 2^2, \dots, 2^{n-1}.$$

Golomb [Ref. 8:p. 76] provides a proof of Theorem III.1. Note that the multipliers which exist for M-sequences are not guaranteed by the Multiplier Theorem II.1.

The multiplier group of all M-sequences with a period of $v = 2^n - 1$ is the group $G = \{1, 2, 2^2, \dots, 2^{n-1}\}$. The cyclotomic cosets of an M-sequence can be created by choosing each residue r , modulo v , and forming the sets

$$Gr = \{r, 2r, 2^2r, \dots, 2^{n-1}r\} \pmod{v}.$$

The number of cyclotomic cosets for an M-sequence having period $v = 2^n - 1$, is given by [Ref. 8:pp. 77-78] as

$$Y(v) = 1/n \sum_{i=1}^n [2^{(i,n)} - 1]$$

where (i,n) is the greatest common divisor of i and n . For the case $n = 3$, the $Y(7) = 3$ cyclotomic cosets are:

$$C_0 = \{0\}$$

$$C_1 = \{1, 2, 4\}$$

$$C_2 = \{3, 6, 5\}.$$

D. DECIMATION

Given a sequence $\{s_k\}$ and any integer $d \geq 1$, the sequence formed by taking every d^{th} term, modulo v , from $\{s_k\}$ is called the d^{th} decimation of $\{s_k\}$. The following examples illustrate some of the decimations of a given M-sequence with period $v = 15$:

$$\begin{aligned} \{s_k\} &= 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \\ \{s_{2k}\} &= 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \\ \{s_{4k}\} &= 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \\ \{s_{8k}\} &= 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \\ \{s_{16k}\} &= 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0. \end{aligned}$$

There are three cyclically shifted versions of $\{s_k\}$ which have particularly interesting decimations. Let $\{s_{k+\tau}\}$ be the sequence obtained by cyclically shifting $\{s_k\}$ by τ positions to the left, then the three cyclic shifts of $\{s_k\}$ and their decimations are:

$$\begin{aligned}
 \{s_{k+14}\} &= 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \\
 \{s_2(k+14)\} &= 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \\
 \{s_{k+4}\} &= 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \\
 \{s_2(k+4)\} &= 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \\
 \{s_4(k+4)\} &= 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \\
 \\
 \{s_{k+9}\} &= 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \\
 \{s_2(k+9)\} &= 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \\
 \{s_4(k+9)\} &= 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1.
 \end{aligned}$$

The following points should be observed:

- (i) $\{s_{k+14}\} = \{s_2(k+14)\}$
- (ii) $\{s_{k+4}\} = \{s_2(k+9)\}$, $\{s_{k+9}\} = \{s_2(k+4)\}$
- (iii) $\{s_{k+4}\} = \{s_4(k+4)\}$, $\{s_{k+9}\} = \{s_4(k+9)\}$.

Other decimations of $\{s_k\}$ by 3, 5 and 7 are:

$$\{s_{3k}\} = 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0$$

$$\{s_{5k}\} = 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0$$

$$\{s_{7k}\} = 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1.$$

Theorem III.1 states that $\{s_{qk}\}$ is equivalent to a cyclically shifted version of $\{s_k\}$ only for $q = 1, 2, \dots, 2^{n-1}$ and this is demonstrated in the example involving the decimations of $\{s_k\}$ by elements in the multiplier group. The sequence $\{s_{k+14}\}$ is the characteristic shift of $\{s_k\}$ since $\{s_{k+14}\} = \{s_{2(k+14)}\}$. In the examples involving the decimations of $\{s_k\}$ by 3 and 5 the resulting sequences have periods which are less than 15. This short cycling occurs due to the fact that 3 and 5 are not relatively prime to 15. The following corollary pertains directly to the last example involving the 7th decimation of $\{s_k\}$.

Corollary III.2

Any M-sequence with period $v = 2^n - 1$ can be derived from any other M-sequence having the same period v by a suitable decimation.

McEliece [Ref. 3:p. 163] provides a complete proof of corollary III.2.

There are only two cyclically distinct M-sequences having period $v = 15$. The 7th decimation of the M-sequence $\{s_k\}$ results in the only other cyclically inequivalent M-

sequence having period $v = 15$. It should be noted that the decimation of $\{s_k\}$ by any two numbers which are in the same cyclotomic coset result in cyclically shifted versions of the same sequence. This means that the decimation of $\{s_k\}$ by 14, 13 and 11 results in cyclically shifted versions of

$$\{s_{7k}\} = 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1$$

which is seen in the following decimations:

$$\{s_{14k}\} = 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1$$

$$\{s_{13k}\} = 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1$$

$$\{s_{11k}\} = 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0.$$

E. TRACE

The concept of trace in a finite field $E = GF(q^n)$ is a particularly useful tool in the analysis of M-sequences. The trace of $\alpha \in E = GF(q^n)$ over the subfield $F = GF(q)$ is defined as

$$\text{Tr}_F^E(\alpha) = \alpha + \alpha q + \alpha q^2 + \alpha q^3 + \dots + \alpha q^{n-1}.$$

If F is the prime subfield of E then $\text{Tr}_F^E(\alpha)$ is called the absolute trace of α and is denoted by $\text{Tr}(\alpha)$. The term trace will denote the absolute trace unless otherwise specified.

The trace of $\alpha \in E = GF(q^n)$ over $F = GF(q)$ is the sum of the conjugates of α with respect to F [Ref. 5:pp. 54-55]. The following theorem gives some of the properties of the trace function.

Theorem III.3

If $\alpha, \beta \in E = GF(q^n)$ and $\rho \in F = GF(q)$, then

- (a) $\text{Tr}(\alpha) \in F$
- (b) $\text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$
- (c) $\text{Tr}(\rho\alpha) = \rho \text{Tr}(\alpha)$
- (d) $\text{Tr}(\alpha^q) = \text{Tr}(\alpha)$
- (e) Tr maps E onto F .

McEliece [Ref. 3:p. 99] provides a proof of theorem III.3. Simply stated, the trace function is a linear transformation from $E = GF(q^n)$ onto $F = GF(q)$.

As an example, let $E = GF(2^4)$ and $F = GF(2)$ with E defined over F by the characteristic polynomial

$$c(x) = x^4 - x - 1 \quad (3.2)$$

Let α be a primitive root of the characteristic polynomial $c(x)$ defined by equation 3.2 so that

$$\alpha^4 = \alpha + 1. \quad (3.3)$$

The elements α^i of the multiplicative group of non-zero elements in $E = GF(2^4)$ can then be generated using equation 3.3. The non-zero elements of $E = GF(2^4)$ and their trace values are listed in Table III.1.

Since every element of $E = GF(2^4)$ can be expressed as a linear combination of α^0 , α^1 , α^2 , and α^3 , the formal calculation of the trace need only be made for these particular elements as follows:

$$\text{Tr}(\alpha^0) = 1+1^2+1^4+1^8 = 0$$

$$\text{Tr}(\alpha^1) = \alpha+\alpha^2+\alpha^4+\alpha^8 = \alpha+\alpha^2+(\alpha+1)+(\alpha^2+1) = 0$$

$$\text{Tr}(\alpha^3) = \alpha^3+\alpha^6+\alpha^{12}+\alpha^9 = \alpha^3+(\alpha^3+\alpha^2)+(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha) = 1$$

Theorem III.3 is then utilized to calculate the trace of the remaining elements of E . For example, the trace of α^{11} is

$$\text{Tr}(\alpha^{11}) = \text{Tr}(\alpha^3+\alpha^2+\alpha) = \text{Tr}(\alpha^3)+\text{Tr}(\alpha^2)+\text{Tr}(\alpha) = 1+0+0 = 1.$$

The characteristic shift of an M-sequence having period $v = 2^n-1$ and characteristic polynomial $c(x)$ can be constructed by means of the trace function as follows [Ref. 3:pp. 160-161]:

$$\text{Tr}(\alpha^0), \text{Tr}(\alpha^1), \text{Tr}(\alpha^2), \dots, \text{Tr}(\alpha^{v-2}), \text{Tr}(\alpha^{v-1}).$$

TABLE III.1
NON-ZERO ELEMENTS OF $E = GF(2^4)$

α^i	$Tr(\alpha^i)$
$\alpha^0 = 1$	$Tr(\alpha^0) = 0$
$\alpha^1 = \alpha$	$Tr(\alpha^1) = 0$
$\alpha^2 = \alpha^2$	$Tr(\alpha^2) = 0$
$\alpha^3 = \alpha^3$	$Tr(\alpha^3) = 1$
$\alpha^4 = \alpha + 1$	$Tr(\alpha^4) = 0$
$\alpha^5 = \alpha^2 + \alpha$	$Tr(\alpha^5) = 0$
$\alpha^6 = \alpha^3 + \alpha^2$	$Tr(\alpha^6) = 1$
$\alpha^7 = \alpha^3 + \alpha + 1$	$Tr(\alpha^7) = 1$
$\alpha^8 = \alpha^2 + 1$	$Tr(\alpha^8) = 0$
$\alpha^9 = \alpha^3 + \alpha$	$Tr(\alpha^9) = 1$
$\alpha^{10} = \alpha^2 + \alpha + 1$	$Tr(\alpha^{10}) = 0$
$\alpha^{11} = \alpha^3 + \alpha^2 +$	$Tr(\alpha^{11}) = 1$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$	$Tr(\alpha^{12}) = 1$
$\alpha^{13} = \alpha^3 + \alpha^2 + 1$	$Tr(\alpha^{13}) = 1$
$\alpha^{14} = \alpha^3 + 1$	$Tr(\alpha^{14}) = 1$

The element α is the primitive root of $c(x)$ which determines the multiplicative group of the finite field $E = GF(2^n)$. Hence, the sequence

$$\{s_i\} = 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1$$

where the elements of $\{s_i\}$ are determined by

$$s_i = \text{Tr}(\alpha^i) \quad i = 0, 1, 2, \dots, 14$$

is the characteristic shift of the M-sequence defined by the characteristic polynomial

$$c(x) = x^4 - x - 1$$

Theorem III.3 gives the relationship of the trace function among all the elements α^k in $E = GF(2^n)$ whose exponents k are in a particular cyclotomic coset of the M-sequence determined by the characteristic polynomial $c(x)$ of E . The cyclotomic cosets of an M-sequence, determined by a characteristic polynomial $c(x)$ and having a period of v , are formed from the cycles of the permutation $i \rightarrow 2i \pmod{v}$ by Theorem III.1. Clearly, all the elements of a particular cyclotomic coset are of the form $2^k i \pmod{v}$. Now by Theorem III.3, $\text{Tr}(\alpha^i) = \text{Tr}((\alpha^i)^2)$ for $\alpha^i \in E = GF(2^n)$ defined by $c(x)$ which implies that

$$\text{Tr}(\alpha^i) = \text{Tr}((\alpha^i)^2) = \dots = \text{Tr}((\alpha^i)^{2^k}) = \text{Tr}(\alpha^{i2^k}).$$

Therefore, $\text{Tr}(\alpha^i) = \text{Tr}(\alpha^j)$ if i and j are elements of the same cyclotomic coset. This essentially means that the conjugates of α^i in E , relative to $F = \text{GF}(2)$, all have the same trace value.

F. SHIFT AND ADD PROPERTY

M-sequences also satisfy the shift and add property which is given in the following theorem.

Theorem III.4

Let $\{S_k\}$ be an M-sequence with period $v = 2^n - 1$. Then for any integer $\tau \neq 0$, modulo v , there exists a unique integer σ , with $1 \leq \sigma \leq v-1$ such that

$$\{s_k\} + \{s_{k+\tau}\} = \{s_{k+\sigma}\}.$$

The sequences are added component-wise modulo 2.

McEliece [Ref. 3:pp. 159-160] provides a proof of theorem III.4. The sequences $\{s_{k+\tau}\}$ and $\{s_{k+\sigma}\}$ are called a shift and add pair. The following example illustrates this important property:

$$\{s_k\} = 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1$$

$$\{s_{k+4}\} = \underline{1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0}$$

$$\{s_{k+5}\} = 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1$$

Clearly,

$$\{s_k\} + \{s_{k+4}\} = \{s_{k+5}\}$$

and this relationship holds for any cyclically shifted version of $\{s_k\}$. The sequences $\{s_{k+4}\}$ and $\{s_{k+5}\}$ are a shift and add pair and the numbers 4 and 5 are also referred to as a shift and add pair relative to $\{s_k\}$. The shift and add property applies in a similar fashion to the non-zero elements in the multiplicative group of $E = GF(2^n)$. The finite field E is determined by the characteristic polynomial of the associated M-sequence. Let α^k be an element in the multiplicative group of non-zero elements in $E = GF(2^n)$ then the shift and add property provides that

$$\alpha^k + \alpha^{k+\tau} = \alpha^{k+\sigma}$$

for a unique pair of integers τ and σ modulo $v = 2^n - 1$, i.e. the elements $\alpha^{k+\tau}$ and $\alpha^{k+\sigma}$ are a shift and add pair.

The values that occupy the positions of a shift and add pair in an M-sequence are related by the following theorem.

Theorem III.5

If α^i and α^j are a shift and add pair in $E = GF(2^n)$ defined by the characteristic polynomial $c(x)$, then

$$(a) \quad \text{Tr}(\alpha^{i+t}) = \text{Tr}(\alpha^{j+t}) \text{ iff } \text{Tr}(\alpha^t) = 0$$

$$(b) \quad \text{Tr}(\alpha^{i+t}) \neq \text{Tr}(\alpha^{j+t}) \text{ iff } \text{Tr}(\alpha^t) = 1$$

where $\alpha^t \in E$.

Proof:

Since α^i and α^j are a shift and add pair, this implies that

$$\alpha^{i+t} + \alpha^{j+t} = \alpha^t.$$

By Theorem III.3

$$\text{Tr}(\alpha^{i+t+\alpha^{j+t}}) = \text{Tr}(\alpha^{i+t}) + \text{Tr}(\alpha^{j+t}) = \text{Tr}(\alpha^t).$$

Clearly,

$$\text{Tr}(\alpha^{i+t}) = \text{Tr}(\alpha^{j+t}) \text{ iff } \text{Tr}(\alpha^t) = 0$$

$$\text{Tr}(\alpha^{i+t}) \neq \text{Tr}(\alpha^{j+t}) \text{ iff } \text{Tr}(\alpha^t) = 1.$$

Theorem III.5 implies that for an M-sequence in a particular cyclic shift relative to the characteristic shift, the values that occupy the positions of a shift and add pair

depend upon the value of the sequence bit in the initial position. For example, the sequence $\{s_k\}$ generated by the characteristic polynomial defined by equation (3.2) is

$$\{s_k\} = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0.$$

The positions of $\{s_k\}$ are indexed by $0, 1, 2, \dots, 14$. The associated shift and add pairs (i, j) for the sequence $\{s_k\}$ are determined by Table III.1 and provided in the following list:

$$\begin{array}{cccc} (1, 4) & (3, 14) & (6, 13) & (12, 11) \\ (2, 8) & (5, 10) & (9, 7) & \end{array}$$

The value in the initial position of $\{s_k\}$ is 0. Therefore the values that occupy positions of any shift and add pair in $\{s_k\}$ must be identical as observed. If $\{s_k\}$ is cyclically shifted by 1 to obtain

$$\{s_{k+1}\} = 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0$$

then the initial position of $\{s_{k+1}\}$ has a value of 1. Consequently, the values that occupy corresponding positions of any shift and add pair must necessarily be unequal, i.e., they are binary complements. For instance, the values

occupying the corresponding positions of the shift and add pair (3,14) are 1 and 0 respectively.

G. REGULARITIES IN CROSS-CORRELATION

Given two uniform M-sequences $\{a_k\}$ and $\{b_k\}$ with a period of v , the cross-correlation function is defined as

$$C(\tau) = \sum_{k=1}^v a_k b_{k+\tau}$$

In the case $\{a_k\} = \{b_{k+\tau}\}$, then the cross-correlation function is the auto-correlation function $C_a(\tau)$ of $\{a_k\}$ as defined earlier. The auto-correlation function will have exactly two values. The number of values taken on by the cross-correlation of two cyclically distinct uniform M-sequences will take on at least three values. The only general statement that can be made about the cross-correlation of two M-sequences is given by the following theorem.

Theorem III.6

The number of distinct values assumed by the cross-correlation function $C(\tau)$ of two M-sequences, $\{a_k\}$ and $\{b_k\}$, both having a period of v , can never exceed $Y(v)$, the number of cyclotomic cosets, modulo v .

Proof:

The proof is reproduced from Golomb [Ref. 8: p. 82]. Without loss of generality, let $\{a_k\}$ and $\{b_k\}$ be

in their characteristic shifts. Now by corollary

III.2

$$\{a_{qk}\} = \{b_k\}$$

for some q , with $(q, v) = 1$. Hence,

$$C(\tau) = \sum_{k=1}^v a_k b_{k+\tau} = \sum_{k=1}^v a_k a_{qk+\tau}$$

By the formula of Gauss for the multiplication of cyclotomic cosets, the value of $C(\tau)$ depends only on the coset to which τ belongs. Therefore the number of different values assumed by $C(\tau)$ can not exceed $Y(v)$, the number of distinct cyclotomic cosets, modulo v .

It is observed that certain regularities exist other than the one indicated by Theorem III.6. In fact it happens on occasion that the cross-correlation function of cyclically distinct M-sequences assumes only three values, which is the minimum number possible. $C(\tau)$ also takes on the values of sequential integers in certain cases. The following examples show these particular regularities:

$$\begin{aligned} \{a_k\} = & 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \\ & 0 \ 1 \ 0 \ 0 \ 0 \ 0 \end{aligned}$$

$$\{b_k\} = 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \\ 0 \ 0 \ 1 \ 0 \ 1 \ 1$$

$$C(\tau) \in \{6, 8, 10\}, \quad v = 31, \quad Y(31) = 7, \quad \{b_k\} = \{a_{5k}\}$$

$$\{a_k\} = 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \\ 0 \ 1 \ 0 \ 0 \ 0 \ 0$$

$$\{b_k\} = 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \\ 1 \ 1 \ 0 \ 1 \ 1 \ 1$$

$$C(\tau) \in \{6, 7, 8, 9, 10, 11\}, \quad Y(31) = 7, \quad \{b_k\} = \{a_{30k}\}$$

The following theorems explicitly determine the cross-correlation function of uniform M-sequences in certain restricted cases. These theorems are presented without proof. A list of references which contain various parts of the proofs of these composite results can be found in Sarwate and Pursley [Ref. 9:p. 603].

Theorem III.7

Let $\{a_i\}$ and $\{b_i\}$ be uniform M-sequences having a period of $2^n - 1$ with $\{b_i\} = \{a_{qi}\}$, where either $q = 2^{k+1}$ or $q = 2^{2k-2^{k+1}}$. If $e = \gcd(n, k)$ is such that n/e is odd, then the cross-correlation function of $\{a_i\}$ and $\{b_i\}$ is three-valued and

$$\begin{aligned} -1+2((n+e)/2) & \text{ occurs } 2^{(n-e-1)+2((n-e-2)/2)} \text{ times,} \\ -1 & \text{ occurs } 2^{n-2(n-e)-1} \text{ times and} \\ -1-2(n+e) & \text{ occurs } 2^{(n-e-1)-2((n-e-2)/2)} \text{ times.} \end{aligned}$$

Theorem III.7 applies to the previous example involving the cross-correlation of the M-sequences having a period of 31 where

[illegible]

and

$$\{b_i\} = 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \\ 0 \ 0 \ 1 \ 0 \ 1 \ 1.$$

These sequences are transformed to their corresponding sequences of 1's and -1's as described in Section II.D and their cross-correlation function is evaluated.

$$\{\mathbf{x}_1\} = \begin{matrix} -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 \end{matrix}$$

$$\{x_i^*\} = \begin{matrix} -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \end{matrix}$$

In this case $n = 5$, $k = 2$, and $q = 13$ so that $\{a_i\} = \{b_{13i}\}$ except for a cyclic shift. Clearly, $e = \gcd(5, 2) = 1$ and $5/1 = 5$ is odd, hence

3 occurs 10 times,
 -1 occurs 15 times and
 -9 occurs 6 times

as actually observed in the computation of $C(\tau)$. A pair of M-sequences which have a three-valued cross-correlation function is called a "preferred" pair.

Theorem III.8

Let $\{a_i\}$ and $\{b_i\}$ denote M-sequences of period $2^n - 1$ where n is a multiple of 4. If $\{a_i\} = \{b_{t(n)i}\}$ with

$$t(n) = 2^{((n+2)/2)} - 1$$

then the cross-correlation function of $\{a_i\}$ and $\{b_i\}$ is four-valued and

$-1 + 2^{((n+2)/2)}$ occurs $(2^{(n-1)} - 2^{((n-2)/2)})/3$ times,
 $-1 + 2^{(n/2)}$ occurs $2^{(n/2)}$ times,
 -1 occurs $2^{(n-1)} - 2^{((n-2)/2)} - 1$ times and
 $-1 - 2^{(n/2)}$ occurs $(2^n - 2^{(n/2)})/3$ times.

Theorem III.8 applies to the following example of the cross-correlation function of M-sequences having a period of 15 with

$$\{a_i\} = 1 \ 1 \ 1 \ -1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1 \ -1 \ -1 \ -1 \ -1$$

and

$$\{b_i\} = 1 \ 1 \ 1 \ -1 \ -1 \ -1 \ -1 \ 1 \ -1 \ 1 \ -1 \ -1 \ 1 \ 1 \ -1.$$

For this example $n = 4$, $t(4) = 7$ and $\{a_i\} = \{b_{7i}\}$, therefore

7 occurs 2 times,
3 occurs 4 times,
-1 occurs 5 times and
-5 occurs 4 times

which agrees with the actual computation of $C(\tau)$.

Theorems III.7 and III.8 indicate when the number of values assumed by the cross-correlation function of two cyclically distinct M-sequences is minimal or near minimal. However, the upper bound on the number of cross-correlation values does not appear to be approached unless $\{a_i\}$ and $\{b_i\}$ are reverse sequences, i.e., $\{a_i\}$ is a cyclically shifted version of $\{b_i\}$ in reverse order [Ref. 8:pp. 82-85].

IV. METHODOLOGY

A. PROCEDURE

This investigation focuses on the cross-correlation functions involving a sample of uniform cyclic difference set sequences generated from a list of cyclic difference sets provided by Baumert [Ref. 1:pp. 150-158]. This list containing the 85 cyclic difference sets for which $k \leq 100$ includes the multipliers and classifications of each cyclic difference set. The cross-correlations are separated into three different categories and each category is treated individually as discussed in the following sections.

Only one cyclic difference set sequence from each complementary pair is necessary for the purposes of this investigation. This is seen by noting that if $\{a_k\}$ is a cyclic difference set sequence composed of 1's and -1's, then the associated complementary sequence $\{\overline{a_k}\}$ is obtained from $\{a_k\}$ by changing the 1's to -1's and vice versa, i.e., $\{\overline{a_k}\} = \{-a_k\}$. The cross-correlation function $C(\tau)$ of the uniform sequences $\{a_k\}$ and $\{b_k\}$ having a period of v is

$$C(\tau) = \sum_{k=1}^v a_k b_{k+\tau}$$

where the subscripts are taken modulo v . The cross-correlation function of the complementary sequence $\{\overline{a_k}\}$ and the sequence $\{b_k\}$ is

$$C(\tau) = \sum_{k=1}^v \overline{a_k} b_{k+\tau} = \sum_{k=1}^v -a_k b_{k+\tau} = - \sum_{k=1}^v a_k b_{k+\tau}$$

Hence, the cross-correlation function of $\{a_k\}$ and $\{b_k\}$ is the negative of $C(\tau)$ for $\{a_k\}$ and $\{b_k\}$.

Table IV.1 identifies the 39 cyclic difference sets used to construct the sample of cyclic difference set sequences. The classifications and multipliers are also provided for each cyclic difference set in the table. The cyclic difference sets with identical parameters are distinguished by the letters A, B, C, ..., etc. The following classification codes are defined as:

- Sn - Hyperplanes in Projective n Space
- L - Quadratic Residues
- TP - Twin Prime Sets
- H - Hall's Sets
- GMW - Gordon, Mills, Welch
- * - No Special Category Applies

A complete enumeration of the elements of each cyclic difference set in Table IV.1 is listed in Appendix A.

TABLE IV.1
SAMPLE CYCLIC DIFFERENCE SETS

(v, k, λ)	CLASSIFICATION	MULTIPLIER
(7, 3, 1)	S2, L	2
(11, 5, 2)	L	3
(15, 7, 3)	S3, TP	2
(19, 9, 4)	L	5
(21, 5, 1)	S2	2
(23, 11, 5)	L	2
(31, 6, 1)	S2	5
(31A, 15, 7)	S4, H	2
(31B, 15, 7)	L	2
(35, 17, 8)	TP	3
(40, 13, 4)	S3	3
(43A, 21, 10)	H	11
(43B, 21, 10)	L	11
(47, 23, 11)	L	2
(57, 8, 1)	S2	7
(59, 29, 14)	L	3
(63A, 31, 15)	S5	2
(63B, 31, 15)	GMW	2
(67, 33, 16)	L	17
(71, 35, 17)	L	2
(79, 39, 19)	L	2
(83, 41, 20)	L	3
(85, 21, 5)	S3	2
(91, 10, 1)	S2	3
(103, 51, 25)	L	2
(107, 53, 26)	L	3
(121A, 40, 13)	S4	3
(121B, 40, 13)	*	3
(121C, 40, 13)	*	3
(121D, 40, 13)	*	3
(127A, 63, 31)	L	2
(127B, 63, 31)	H	2
(127C, 63, 31)	S6	2
(127D, 63, 31)	*	2
(127E, 63, 31)	*	2
(127F, 63, 31)	*	2
(131, 65, 32)	L	3
(133, 12, 1)	S2	11
(133, 33, 8)	*	5

1. Sample Construction

The sample of 39 cyclic difference sets is derived from the list of cyclic difference sets provided by Baumert. The corresponding cyclic difference set sequences are generated by the characteristic function of each cyclic difference set. These cyclic difference set sequences $\{s_k\}$ of 0's and 1's are then transformed into sequences $\{x_k\}$ of 1's and -1's by

$$x_k = 1 - 2s_k.$$

The cross-correlation functions are evaluated using these sequences of 1's and -1's.

2. Span

The span of a periodic binary sequence $\{s_k\}$ is defined as the smallest positive integer n such that all subsequences of length n in $\{s_k\}$ are unique. The span of each cyclic difference set sequence in the sample is determined by an exhaustive computer search and is provided in Appendix A.

B. CYCLOTOMIC COSETS AND EQUIVALENT SEQUENCES

The multipliers of the cyclic difference set sequences with period v are used to construct the associated cyclotomic cosets, modulo v , for each sequence in the sample. The multiplier group G is formed from the multipliers of each sequence. The cosets are determined by

forming the products $rG \pmod v$ where r is an arbitrary residue, modulo v , as noted in Section II.F.

The cosets described above are utilized to obtain the equivalent sequences of a given cyclic difference set sequence $\{a_k\}$. Recall that two cyclic (v, k, λ) -difference sets D_k and D_j are said to be equivalent if $D_k = qD_j + z$ for some integers q and z with q relatively prime to v . Analogously, two uniform cyclic difference set sequences $\{a_k\}$ and $\{b_k\}$ having a period of v are said to be equivalent if $\{a_k\} = \{b_{qk+z}\}$ for some integers q and z with q relatively prime to v . Consequently, all the cyclic difference set sequences equivalent to the cyclic difference set sequence $\{b_k\}$ are obtained by properly decimating $\{b_k\}$. A proper decimation is defined as a decimation by an integer relatively prime to v .

Decimating any cyclic difference set sequence by integers which are in the same cyclotomic coset results in cyclically shifted versions of the same sequence. Without loss of generality, only one cyclic difference set sequence from each class of coset decimations are considered. Therefore, a sequence $\{b_k\}$ need only be decimated by one representative element from each coset containing integers which are relatively prime to v . This produces one each of the sequences equivalent to $\{b_k\}$, none of which are cyclic shifts of any another.

The cyclotomic cosets associated with each sequence in the sample are provided in Appendix B, except for the Hadamard quadratic residue sequences. The cyclotomic cosets are referenced by the period and multipliers of the corresponding sequences. The cyclotomic cosets for the Hadamard quadratic residue sequences are shown to have a very structured form in a later section which precludes the necessity of listing them explicitly.

D. CROSS-CORRELATION

The cross-correlation function $C(\tau)$ is evaluated for the uniform cyclic difference set sequences in the sample. In nearly all of the cases, only the number of values assumed by $C(\tau)$ is described. In the special cases involving the cross-correlations of equivalent quadratic residue sequences, the actual values assumed by $C(\tau)$ are also included.

There are two major types of cross-correlations that are evaluated. One type pertains to the cross-correlation of equivalent sequences and the other pertains to the cross-correlation of inequivalent sequences. A pair of cyclic difference set sequences $\{a_k\}$ and $\{b_k\}$ are inequivalent if one is not a cyclically shifted decimation of the other, i.e., $\{a_k\} \neq \{b_{qk+\tau}\}$. These two types of cross-correlations are treated separately. The cross-correlations involving equivalent Hadamard quadratic residue sequences are treated as a special category.

1. Equivalent Sequences

A set of cyclically distinct, equivalent sequences are derived for each cyclic difference set sequence in the sample. This is accomplished by properly decimating each of the sample sequences as discussed in Section IV.B. The original cyclic difference set sequence from the sample is then cross-correlated with each of its equivalent decimations.

2. Inequivalent Sequences

There are only 19 cyclic difference set sequences from the sample for which cross-correlations between inequivalent uniform sequences are possible. In order to evaluate a cross-correlation of uniform inequivalent cyclic difference set sequences, at least two uniform inequivalent sequences are required. Consequently, all the cyclic difference set sequences having a unique period in the sample are excluded from consideration. This leaves 19 inequivalent cyclic difference set sequences for the investigation. Table IV.2 provides the number of sequences having each of the indicated periods which appear among the 19 cyclic difference set sequences.

There are 3 inequivalent sequences in the sample having a period of 31. Hence, there are 3 possible combinations of these particular inequivalent sequences which can be cross-correlated. The total number of possible cross-correlations involving uniform inequivalent sequences

TABLE IV.2
PERIOD DISTRIBUTION OF INEQUIVALENT SEQUENCES

<u>Period</u>	<u>No. of Sequences</u>
31	3
43	2
63	2
121	4
127	6
133	2

from this sample is 27, as determined by Table IV.2. All 27 cross-correlations are evaluated in this investigation.

3. M-Sequences

The M-sequences having periods 15, 31, 63, and 127 are each represented in the sample by an equivalent binary complement. Every M-sequence of period v can be obtained by a suitable decimation of any M-sequence of period v by Corollary III.2. Therefore, properly decimating a particular binary complement of an M-sequence results in a sequence which is the binary complement of another cyclically distinct M-sequence.

The sequences generated from the following cyclic difference sets are binary complements of the M-sequences which have the indicated characteristic polynomial $c(x)$:

(15,7,3)	S3,TP	$c(x) = x^4 - x - 1$
(31A,15,7)	S4,H	$c(x) = x^5 - x^3 - 1$

(63A,31,15)	S5	$c(x) = x^6 - x - 1$
(127C,63,31)	S6	$c(x) = x^7 - x^5 - x^2 - x - 1$

The corresponding complementary cyclic difference sets have parameters (v, k, λ) :

$$\begin{aligned} &(15, 8, 4) \\ &(31, 16, 8) \\ &(63, 32, 16) \\ &(127, 64, 32) \end{aligned}$$

which are of the form $(2^n - 1, 2^{n-1}, 2^{n-2})$. These parameters coincide with the parameters of the cyclic difference sets associated with M-sequences as noted in Section II.B.

Proper decimations of each previously listed "complementary" M-sequence result in binary complements of all the respective M-sequences for a given period. For example, in the case of the cyclic difference set

$$D = \{0, 1, 2, 4, 5, 8, 10\} \quad (v, k, \lambda) = (15, 7, 3)$$

the associated cyclic difference set sequence is

$$\{s_k\} = 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0.$$

The sequence $\{s_k\}$ is the complementary sequence of the M-sequence

$$\{\overline{s_k}\} = 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1$$

defined by the characteristic polynomial

$$c(x) = x^4 - x - 1.$$

If the 7th decimation of $\{s_k\}$ is formed

$$\{\overline{s_{7k}}\} = 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1,$$

it is the complementary sequence of the only other cyclically distinct M-sequence of period 15

$$\{s_{7k}\} = 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0,$$

defined by the characteristic polynomial

$$c(x) = x^4 - x^3 - 1.$$

As stated previously in Section IV.A, only one sequence from a complementary pair need be considered in the investigation of the cross-correlation functions of uniform cyclic difference set sequences. Therefore, it is not

necessary to include the cross-correlations of the actual M-sequences themselves having the aforementioned periods.

V. RESULTS

A. REMARKS

The scope of this thesis is essentially limited in most cases to investigating the number of values assumed by the cross-correlation function of uniform cyclic difference set sequences. In the special cases involving the cross-correlations of quadratic residue sequences, the actual values taken on by $C(\tau)$ are also considered. The general observations and results are presented separately for each type of cross-correlation.

B. CROSS-CORRELATION OF INEQUIVALENT SEQUENCES

The number of values assumed by the cross-correlation functions of inequivalent cyclic difference set sequences are provided in a condensed format in Appendix C. Since the sequences are inequivalent they do not necessarily have the same multipliers or the same number of cyclotomic cosets. Therefore, the number of cyclotomic cosets is provided for each inequivalent sequence as determined by their respective multipliers listed in Table IV.1.

The cross-correlations of inequivalent sequences are observed to take on 3 values in only 2 cases and a maximum number of 11 values in 5 cases as listed in Appendix C. The average number of values assumed for these 27 cross-correlations is approximately 8. There are no apparent

regularities discernible to the author among these inequivalent cross-correlations.

C. CROSS-CORRELATION OF EQUIVALENT SEQUENCES

The number of values taken on by the cross-correlation functions of equivalent cyclic difference set sequences are provided in a condensed format in Appendix D. The original sequence from the sample, $\{s_k\}$, is cross-correlated with each of its proper decimations, $\{s_{qk}\}$. The number of cyclotomic cosets is given for $\{s_k\}$ as determined by its multipliers listed in Table IV.1.

The number of values assumed by the cross-correlations of equivalent cyclic difference set sequences are observed not to exceed the number of cyclotomic cosets in all cases. Theorem III.6 states that the number of distinct values assumed by the cross-correlation function of two M-sequences, both of period v , can never exceed the number of cyclotomic cosets, modulo v . This theorem applies in general to equivalent cyclic difference set sequences. The following modified version of Theorem III.6 is presented for this general case.

Theorem V.1

The number of distinct values assumed by the cross-correlation function $C(\tau)$ of two equivalent cyclic difference set sequences, $\{a_k\}$ and $\{b_k\}$, uniform with a

period of v , can never exceed the number of cyclotomic cosets, modulo v .

Proof:

The proof of Theorem V.1 is identical to the proof of Theorem III.6. Since $\{a_k\}$ and $\{b_k\}$ are equivalent cyclic difference set sequences

$$\{a_{qk}\} = \{b_k\}$$

for some q , with $(q, v) = 1$. Without loss of, generality let $\{a_k\}$ and $\{b_k\}$ be in their characteristic shifts.

The cross-correlation function of $\{a_k\}$ and $\{b_k\}$ is

$$C(\tau) = \sum_{k=1}^v a_k b_{k+\tau} = \sum_{k=1}^v a_k a_{qk+\tau}.$$

By the formula of Gauss for the multiplication of cyclotomic cosets, $C(\tau)$ depends only on the coset to which τ belongs. Therefore the number of different values assumed by $C(\tau)$ can not exceed the number of cyclotomic cosets, modulo v .

It is not uncommon for the cross-correlation function of equivalent cyclic difference set sequences to assume exactly 3 values as seen in several cases presented in Appendix D. However, it is not clear when the cross-correlation between equivalent cyclic difference set sequences will take on any

particular number of values except in the cases involving M-sequences as noted in Section III.G. Finally, we observe that the number of values assumed by the cross-correlation of equivalent cyclic difference set sequences never appears to approach the upper bound set by Theorem V.1 unless one sequence is the reverse of the other.

D. CROSS-CORRELATION OF EQUIVALENT QUADRATIC RESIDUE SEQUENCES

There are 16 quadratic residue sequences in the sample identified as follows:

(7,3,1)	(11,5,2)	(19,9,4)	(23,11,5)
(31B,15,7)	(43B,21,10)	(47,23,11)	(59,29,14)
(67,33,16)	(71,35,17)	(79,39,19)	(83,41,20)
(103,51,25)	(107,53,26)	(127A,63,31)	(131,65,32).

Clearly, all of these sequences are of the Hadamard type having parameters $(4t-1, 2t-1, t-1)$.

The quadratic residue sequences have a multiplier group composed of the quadratic residues, modulo v , and each sequence has exactly 3 cyclotomic cosets. The first coset contains the single element 0, the second coset contains the $2t-1$ quadratic residues, modulo v , and the third coset contains the remaining $2t-1$ quadratic non-residues, modulo v .

Consequently, only 1 cyclically distinct equivalent sequence exists for each of the quadratic residue sequences in the sample. The equivalent sequence is obtained by decimating the quadratic residue sequence $\{s_k\}$ by q , a quadratic non-residue, modulo v . Furthermore, $\{s_k\}$ and $\{s_{qk}\}$ are observed to be reverse sequences.

The cross-correlations of $\{s_k\}$ with $\{s_{qk}\}$ assume 3 values in all the observed cases and

$$\begin{aligned} -1 &\text{ occurs } 2t-1 \text{ times,} \\ 3 &\text{ occurs } 2t-1 \text{ times and} \\ -(4t-3) &\text{ occurs } 1 \text{ time.} \end{aligned}$$

For example, in the case of the sequence $\{s_k\}$ identified by its parameters $(23,11,5)$, the equivalent sequence $\{s_{5k}\}$ is obtained by decimating $\{s_k\}$ by 5 which is a quadratic non-residue, modulo 23. The cross-correlation of $\{s_k\}$ with $\{s_{5k}\}$ takes on 3 values and

$$\begin{aligned} -1 &\text{ occurs } 11 \text{ times,} \\ 3 &\text{ occurs } 11 \text{ times and} \\ -21 &\text{ occurs } 1 \text{ time.} \end{aligned}$$

This cross-correlation function shows there is a particular cyclic shift of $\{s_k\}$ for which a strong negative cross-correlation exists between $\{s_k\}$ and $\{s_{qk}\}$. The strong

negative cross-correlation indicates that this particular cyclic shift of $\{s_k\}$ is nearly the binary complement of $\{s_{qk}\}$. In fact, $\{s_k\}$ and $\{s_{qk}\}$ agree in only one position. The observed cross-correlation functions of equivalent quadratic residue sequences suggest the following conjecture.

Conjecture V.2

Let $\{s_k\}$ be a cyclic difference set sequence generated from a quadratic residue set with parameters $v = 4t-1$, $k = 2t-1$, and $\lambda = t-1$ such that v is prime. If $\{s_{qk}\}$ is an equivalent decimation of $\{s_k\}$ by a quadratic non-residue q , modulo v , then the cross-correlation function $C(\tau)$ of $\{s_k\}$ and $\{s_{qk}\}$ is 3 valued and

-1 occurs $2t-1$ times,
 3 occurs $2t-1$ times and
 $-(4t-3)$ occurs 1 time.

Furthermore, let Q be the set of quadratic residues, modulo v , and let N be the set of quadratic non-residues, modulo v . If $C(\tau^*) = -(4t-3)$ for some fixed shift τ^* , then

$$C(\tau^* + \tau) = \begin{cases} -1 & \text{if } \tau \in N \text{ and } \tau \not\equiv 0 \pmod{v} \\ 3 & \text{if } \tau \in Q \\ -(4t-3) & \text{if } \tau \equiv 0 \pmod{v}. \end{cases}$$

Each quadratic residue sequence in the sample is observed to have 3 cyclotomic cosets, namely the single element 0, the quadratic residues, modulo v , and the quadratic non-residues, modulo v . In order to obtain exactly 3 cosets a "proper" multiplier must be chosen.

The multipliers of a quadratic residue cyclic difference set are the quadratic residues themselves by Theorem II.3. For the case $v = 127$, if the multiplier 2 ($16^2 \equiv 2 \pmod{127}$) is selected, then the corresponding multiplier group is

$$G = \{1, 2, 4, 8, 16, 32, 64\}.$$

which clearly does not contain all the quadratic residues, modulo 127. For this example G generates a total of 19 cyclotomic cosets. If on the other hand, the quadratic residue 9 is chosen as the generator of the multiplier group, then G contains all the quadratic residues, modulo 127, and there are a total of 3 cyclotomic cosets.

Theorem V.1 indicates that the number of values taken on by the cross-correlation function of the equivalent quadratic residue sequences in the sample can not exceed 3, as observed in all cases. The following theorem shows that

the cross-correlation function of equivalent quadratic residue sequences never assumes more than three values.

Theorem V.3

Let $\{s_k\}$ be a Hadamard quadratic residue sequence with parameters $v = 4t-1$, $k = 2t-1$ and $\lambda = t-1$ such that v is prime. If $\{s_{dk}\}$ is a decimation of $\{s_k\}$ by a quadratic non-residue d , then the cross-correlation function of $\{s_k\}$ and $\{s_{dk}\}$ takes on a maximum of 3 values.

Proof:

If $v = 4t-1$ is prime then the residues, modulo v , constitute a finite field. Therefore, the multiplicative group of the nonzero residues, modulo v , is cyclic.

Consider the set Q of all quadratic residues, modulo v . Clearly, 1 is an element of Q so that Q is non-empty. If $q_1, q_2 \in Q$, then for some non-zero residues x_1 and x_2 , modulo v ,

$$q_1 \equiv x_1^2 \pmod{v}$$

$$q_2 \equiv x_2^2 \pmod{v}$$

Hence,

$$\begin{aligned} q_1 \cdot q_2 &\equiv x_1^2 \cdot x_2^2 \pmod{v} \\ &\equiv (x_1 \cdot x_2)^2 \pmod{v} \end{aligned}$$

and $(q_1 \cdot q_2) \in Q$. Since the quadratic residues are closed under multiplication, they necessarily form a subgroup of the multiplicative group of non-zero residues, modulo v . Every subgroup of a cyclic group is cyclic therefore Q is cyclic and $Q = \langle q \rangle$ for some $q \in Q$.

By Theorem II.3, the multipliers of a quadratic residue set are the quadratic residues themselves. Let the multiplier group $G = Q$ be generated by the multiplier $q \in Q$ such that

$$G = Q = \{q, q^2, q^3, \dots, q^{2t-2}, q^{2t-1}\} \pmod{v}.$$

Clearly, Q is one particular cyclotomic coset, modulo v . The other cyclotomic cosets are constructed by forming the products $xQ \pmod{v}$ where x is a quadratic non-residue, modulo v . In the trivial case where $x = 0$, the cyclotomic coset contains only the single element 0. We now show that the only remaining cyclotomic coset contains all the non-zero quadratic non-residues, modulo v .

Let x be a non-zero quadratic non-residue, modulo v , and consider

$$N = xQ = \{xq, xq^2, xq^3, \dots, xq^{2t-2}, xq^{2t-1}\} \pmod{v}.$$

Suppose $|N| < 2t-1$, then

$$xq^i \equiv xq^j \pmod{v} \quad \text{for } 1 \leq i < j \leq 2t-1$$

Therefore,

$$xq^i = kv + xq^j \quad k \in \mathbb{Z}$$

$$kv = x(q^j - q^i)$$

$$v = x(q^j - q^i)/k \quad k \neq 0.$$

Since v is prime, either

$$(i) \quad x = v \text{ and } q^j - q^i = k$$

or

$$(ii) \quad x = k \text{ and } q^j - q^i = v \text{ must hold.}$$

Case (i): If $x = v$ then $x \equiv 0 \pmod{v}$ so that $xQ = \{0\}$ which has been previously discussed and is not under consideration.

Case (ii): If $q^j - q^i = v$ then $q^j \equiv q^i \pmod{v}$ which is clearly a contradiction. Hence, the $4t-1$ residues, modulo v , have been accounted for in exactly 3 cyclotomic cosets as follows:

$$C_0 = \{0\}$$

$$C_1 = \{q, q^2, q^3, \dots, q^{2t-2}, q^{2t-1}\} \pmod{v}$$

$$C_2 = \{xq, xq^2, xq^3, \dots, xq^{2t-2}, xq^{2t-1}\} \pmod{v}$$

where q is a quadratic residue such that $Q = \langle q \rangle$ and x is a non-zero quadratic non-residue, modulo v .

Therefore, the cross-correlation function of equivalent Hadamard quadratic residue sets can not assume more than 3 values by Theorem V.1.

It is not clear to the author why the cross-correlation functions of equivalent quadratic residue sequences assume the 3 particular observed values.

VI. CONCLUSIONS

The maximum number of values assumed by the cross-correlation function of equivalent cyclic difference set sequences is shown to be bounded. This upper bound is the number of cyclotomic cosets, modulo v , for uniform equivalent cyclic difference set sequences having a period of v . In certain special cases involving M-sequences, the cross-correlation function is known to take on three and four explicit values with stipulated frequencies of occurrence, as given by existing theorems.

The cross-correlation of equivalent Hadamard quadratic residue sequences is conjectured to take on three specified values. In each cross-correlation involving equivalent Hadamard quadratic residue sequences having the associated parameters $v = 4t-1$, $k = 2t-1$, and $\lambda = t-1$, it is observed that

-1 occurs $2t-1$ times,

3 occurs $2t-1$ times and

$-(4t-3)$ occurs 1 time.

In partial support of the conjecture, it is shown that the number of values assumed by the cross-correlation of

equivalent Hadamard quadratic residue sequences can not exceed three.

The cross-correlations of the uniform inequivalent cyclic difference set sequences assume three values in two separate cases however no distinguishing characteristics are derived by the author from the relatively small sample. It should be mentioned that other inequivalent cross-correlations are possible from the set of 19 inequivalent sequences considered in this investigation. These additional cross-correlations involve properly decimated versions of the 19 inequivalent sequences and may demonstrate some regularities which are not evident in this sample.

APPENDIX A

SAMPLE CYCLIC DIFFERENCE SETS

(v, k, λ)	Span	Cyclic Difference Set
(7,3,1)	3	1, 2, 4
(11,5,2)	5	1, 3, 4, 5, 9
(15,7,3)	4	0, 1, 2, 4, 5, 8, 10
(19,9,4)	5	1, 4, 5, 6, 7, 9, 11, 16, 17
(21,5,1)	9	3, 6, 7, 12, 14
(23,11,5)	7	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18
(31,6,1)	12	1, 5, 11, 24, 25, 27
(31A,15,7)	5	1, 2, 3, 4, 6, 8, 12, 15, 16, 17 23, 24, 27, 29, 30
(31B,15,7)	7	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18 19, 20, 25, 28
(35,17,8)	8	0, 1, 3, 4, 7, 9, 11, 12, 13, 14, 16 17, 21, 27, 28, 29, 33
(40,13,4)	10	1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25 27, 35
(43A,21,10)	8	1, 2, 3, 4, 5, 8, 11, 12, 16, 19, 20 21, 22, 27, 32, 33, 35, 37, 39, 41 42
(43B,21,10)	7	1, 4, 6, 9, 10, 11, 13, 14, 15, 16 17, 21, 23, 24, 25, 31, 35, 36, 38 40, 41
(57,8,1)	18	1, 6, 7, 9, 19, 38, 42, 49
(47,23,11)	9	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16 17, 18, 21, 24, 25, 27, 28, 32, 34 36, 37, 42

(v, k, λ)	Span	Cyclic Difference Set
$(59, 29, 14)$	9	1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19 20, 21, 22, 25, 26, 27, 28, 29, 35 36, 41, 45, 46, 48, 49, 51, 53, 57
$(63A, 31, 15)$	6	0, 1, 2, 3, 4, 6, 7, 8, 9, 12, 13 14, 16, 18, 19, 24, 26, 27, 28, 32 33, 35, 36, 38, 41, 45, 48, 49, 52 54, 56
$(63B, 31, 15)$	11	0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12 16, 17, 18, 20, 23, 24, 27, 29, 32 33, 34, 36, 40, 43, 45, 46, 48, 53 54, 58
$(67, 33, 16)$	8	1, 4, 6, 9, 10, 14, 15, 16, 17, 19 21, 22, 23, 24, 25, 26, 29, 33, 35 36, 37, 39, 40, 47, 49, 54, 55, 56 59, 60, 62, 64, 65
$(71, 35, 17)$	10	1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15 16, 18, 19, 20, 24, 25, 27, 29, 30 32, 36, 37, 38, 40, 43, 45, 48, 49 50, 54, 57, 58, 60, 64
$(79, 39, 19)$	10	1, 2, 4, 5, 8, 9, 10, 11, 13, 16, 18 19, 20, 21, 22, 23, 25, 26, 31, 32 36, 38, 40, 42, 44, 45, 46, 49, 50 51, 52, 55, 62, 64, 65, 67, 72, 73 76
$(83, 41, 20)$	11	1, 3, 4, 7, 9, 10, 11, 12, 16, 17 21, 23, 25, 26, 27, 28, 29, 30, 31 33, 36, 37, 38, 40, 41, 44, 48, 49 51, 59, 61, 63, 64, 65, 68, 69, 70 75, 77, 78, 81
$(85, 21, 5)$	16	0, 1, 2, 4, 7, 8, 14, 16, 17, 23, 27 28, 32, 34, 43, 46, 51, 54, 56, 64 68
$(91, 10, 1)$	25	0, 1, 3, 9, 27, 49, 56, 61, 77, 81
$(103, 51, 25)$	11	1, 2, 4, 7, 8, 9, 13, 14, 15, 16, 17 18, 19, 23, 25, 26, 28, 29, 30, 32 33, 34, 36, 38, 41, 46, 49, 50, 52 55, 56, 58, 59, 60, 61, 63, 64, 66 68, 68, 72, 76, 79, 81, 82, 83, 91 92, 93, 97, 98, 100

(v, k, λ)	Span	Cyclic Difference Set
$(107, 53, 26)$	11	1, 3, 4, 9, 10, 11, 12, 13, 14, 16 19, 23, 25, 27, 29, 30, 33, 34, 35 36, 37, 39, 40, 41, 42, 44, 47, 48 49, 52, 53, 56, 57, 61, 62, 64, 69 75, 76, 79, 81, 83, 85, 86, 87, 89 90, 92, 99, 100, 101, 102, 105
$(121A, 40, 13)$	13	1, 3, 4, 7, 9, 11, 12, 13, 21, 25 27, 33, 34, 36, 39, 44, 55, 63, 64 67, 68, 70, 71, 75, 80, 81, 82, 83 85, 89, 92, 99, 102, 103, 104, 108 109, 115, 117, 119
$(121B, 40, 13)$	12	1, 3, 4, 5, 9, 12, 13, 14, 15, 16 17, 22, 23, 27, 32, 34, 36, 39, 42 45, 46, 48, 51, 64, 66, 69, 71, 77 81, 82, 85, 86, 88, 92, 96, 102, 108 109, 110, 117
$(121C, 40, 13)$	14	1, 3, 4, 7, 8, 9, 12, 21, 24, 25, 26 27, 34, 36, 40, 43, 49, 63, 64, 68 70, 71, 72, 75, 78, 81, 82, 83, 89 92, 94, 95, 97, 102, 104, 108, 112 113, 118, 120
$(121D, 40, 13)$	15	1, 3, 4, 5, 7, 9, 12, 14, 15, 17, 21 27, 32, 36, 38, 42, 45, 46, 51, 53 58, 63, 67, 68, 76, 79, 80, 81, 82 83, 96, 100, 103, 106, 107, 108, 114 115, 116, 119
$(127A, 63, 31)$	15	1, 2, 4, 8, 9, 11, 13, 15, 16, 17 18, 19, 21, 22, 25, 26, 30, 31, 32 34, 35, 36, 37, 38, 41, 42, 44, 47 49, 50, 52, 60, 61, 62, 64, 68, 69 70, 71, 72, 73, 74, 76, 79, 81, 82 84, 87, 88, 94, 98, 99, 100, 103 104, 107, 113, 115, 117, 120, 121 122, 124
$(127B, 63, 31)$	11	1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14 16, 19, 20, 23, 24, 25, 27, 28, 32 33, 38, 40, 46, 47, 48, 50, 51, 54 56, 57, 61, 63, 64, 65, 66, 67, 73 75, 76, 77, 80, 87, 89, 92, 94, 95 96, 97, 100, 101, 102, 107, 108, 111 112, 114, 117, 119, 122, 123, 125 126

(v, k, λ)	Span	Cyclic Difference Set
$(127C, 63, 31)$	7	1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 15 16, 17, 18, 24, 27, 28, 29, 30, 31 32, 34, 36, 39, 47, 48, 51, 54, 56 58, 60, 61, 62, 64, 65, 67, 68, 71 72, 77, 78, 79, 83, 87, 89, 94, 96 97, 99, 102, 103, 105, 107, 108, 112 113, 115, 116, 117, 120, 121, 122, 124
$(127D, 63, 31)$	13	1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14 16, 17, 18, 19, 24, 25, 26, 27, 28 31, 32, 34, 35, 36, 38, 47, 48, 50 51, 52, 54, 56, 61, 62, 64, 65, 67 68, 70, 72, 73, 76, 77, 79, 81, 87 89, 94, 96, 97, 100, 102, 103, 104 107, 108, 112, 115, 117, 121, 122, 124
$(127E, 63, 31)$	12	1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15 16, 17, 18, 19, 20, 24, 25, 27, 29 30, 32, 33, 34, 36, 38, 39, 40, 48 50, 51, 54, 55, 58, 59, 60, 64, 65 66, 68, 71, 72, 73, 76, 77, 78, 80 83, 89, 91, 93, 96, 99, 100, 102 105, 108, 109, 110, 113, 116, 118 120
$(127F, 63, 31)$	15	1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 16 19, 20, 21, 22, 24, 25, 27, 29, 32 33, 37, 38, 39, 40, 41, 42, 44, 48 49, 50, 51, 54, 58, 63, 64, 65, 66 69, 73, 74, 76, 77, 78, 80, 82, 83 84, 88, 89, 95, 96, 98, 100, 102 105, 108, 111, 116, 119, 123, 125 126
$(131, 65, 32)$	11	1, 3, 4, 5, 7, 9, 11, 12, 13, 15, 16 20, 21, 25, 27, 28, 33, 34, 35, 36 38, 39, 41, 43, 44, 45, 46, 48, 49 52, 53, 55, 58, 59, 60, 61, 62, 63 64, 65, 74, 75, 77, 80, 81, 84, 89 91, 94, 99, 100, 101, 102, 105, 107 108, 109, 112, 113, 114, 117, 121 123, 125, 129
$(133, 12, 1)$	42	1, 11, 16, 40, 41, 43, 52, 60, 74 78, 121, 128
$(133, 33, 8)$	17	1, 4, 5, 14, 16, 19, 20, 21, 25, 38 54, 56, 57, 64, 66, 70, 76, 80, 83 84, 91, 93, 95, 98, 100, 101, 105 106, 114, 123, 125, 126, 131

APPENDIX B

CYCLOTOMIC COSETS

Period: 15
Multiplier: 2

COSET

C₀
C₁
C₂
C₃
C₄

ELEMENTS

0
1, 2, 4, 8
3, 6, 12, 9
5, 10
7, 14, 13, 11

Period: 21
Multiplier: 2

COSET

C₀
C₁
C₂
C₃
C₄
C₅

ELEMENTS

0
1, 2, 4, 8, 16, 11
3, 6, 12
5, 10, 20, 19, 17, 13
7, 14
9, 18, 15

Period: 31
Multiplier: 2

COSET

C₀
C₁
C₂
C₃
C₄
C₅
C₆

ELEMENTS

0
1, 2, 4, 8, 16
3, 6, 12, 24, 17
5, 10, 20, 9, 18
15, 30, 29, 27, 23
19, 7, 14, 28, 25
26, 21, 11, 22, 13

Period: 35
Multiplier: 3

COSET

C₀
C₁

C₂

C₃
C₄

ELEMENTS

0
1, 3, 9, 27, 11, 33, 29,
17, 16, 13, 4, 12
2, 6, 18, 19, 22, 31, 23,
34, 32, 26, 8, 24
5, 15, 45, 30, 20, 25
7, 21, 28, 14

Period: 40
Multiplier: 3

COSET

C₀
C₁
C₂
C₃
C₄
C₅
C₆
C₇
C₈
C₉
C₁₀
C₁₁
C₁₂

ELEMENTS

0
1, 3, 9, 27
2, 6, 8, 14
4, 12, 36, 28
5, 15
7, 21, 23, 29
8, 24, 32, 16
10, 30
11, 33, 19, 17
13, 39, 37, 31
20
22, 26, 38, 34
25, 35

Period: 43
Multiplier: 11

COSET

C₀
C₁
C₂
C₃
C₄
C₅
C₆

ELEMENTS

0
1, 11, 35, 41, 21, 16, 4
2, 22, 27, 39, 42, 32, 8
3, 33, 19, 37, 20, 5, 12
6, 23, 38, 31, 40, 10, 24
7, 34, 30, 29, 18, 26, 28
9, 13, 14, 25, 17, 15, 36

Period: 57
Multiplier: 7

<u>COSET</u>	<u>ELEMENTS</u>
C ₀	0
C ₁	1, 7, 49
C ₂	2, 14, 41
C ₃	3, 21, 33
C ₄	4, 28, 25
C ₅	5, 35, 17
C ₆	6, 42, 9
C ₇	8, 56, 50
C ₈	10, 13, 34
C ₉	11, 20, 26
C ₁₀	12, 27, 18
C ₁₁	15, 48, 51
C ₁₂	16, 55, 43
C ₁₃	19
C ₁₄	22, 40, 52
C ₁₅	23, 47, 44
C ₁₆	24, 54, 36
C ₁₇	29, 32, 53
C ₁₈	30, 39, 45
C ₁₉	31, 46, 37
C ₂₀	38

Period: 63
Multiplier: 2

<u>COSET</u>	<u>ELEMENTS</u>
C ₀	0
C ₁	1, 2, 4, 8, 16, 32
C ₂	3, 6, 12, 24, 48, 33
C ₃	5, 10, 20, 40, 17, 34
C ₄	7, 14, 28, 56, 49, 35
C ₅	9, 18, 36
C ₆	11, 22, 44, 25, 50, 37
C ₇	13, 26, 52, 41, 19, 38
C ₈	15, 30, 60, 57, 51, 39
C ₉	21, 42
C ₁₀	23, 46, 29, 58, 53, 43
C ₁₁	27, 54, 45
C ₁₂	31, 62, 61, 59, 55, 47

Period: 85
Multiplier: 2

<u>COSET</u>	<u>ELEMENTS</u>
C ₀	0
C ₁	1, 2, 4, 8, 16, 32, 64, 43
C ₂	3, 6, 12, 24, 48, 11, 22, 44
C ₃	5, 10, 20, 40, 80, 75, 65, 45
C ₄	7, 14, 28, 56, 27, 54, 23, 46
C ₅	9, 18, 36, 72, 59, 33, 66, 47
C ₆	13, 26, 52, 19, 38, 76, 67, 49
C ₇	15, 30, 60, 35, 70, 55, 25, 50
C ₈	17, 34, 68, 51
C ₉	21, 42, 84, 83, 81, 77, 69, 53
C ₁₀	29, 58, 31, 62, 39, 78, 71, 57
C ₁₁	37, 74, 63, 41, 82, 79, 73, 61

Period: 91
Multiplier: 3

<u>COSET</u>	<u>ELEMENTS</u>
C ₀	0
C ₁	1, 3, 9, 27, 81, 61
C ₂	2, 6, 18, 54, 71, 31
C ₃	4, 12, 36, 17, 51, 62
C ₄	5, 15, 45, 44, 41, 32
C ₅	7, 21, 63
C ₆	8, 24, 72, 34, 11, 33
C ₇	10, 30, 90, 88, 82, 64
C ₈	13, 39, 26, 78, 52, 65
C ₉	14, 42, 35
C ₁₀	16, 48, 53, 68, 22, 66
C ₁₁	19, 57, 80, 58, 83, 67
C ₁₂	20, 60, 89, 85, 73, 37
C ₁₃	23, 69, 25, 75, 43, 38
C ₁₄	28, 84, 70, 28, 84, 70
C ₁₅	29, 87, 79, 55, 74, 40
C ₁₆	46, 47, 50, 59, 86, 76

Period: 121
Multiplier: 3

COSET

C₀
C₁
C₂
C₃
C₄
C₅
C₆
C₇
C₈
C₉
C₁₀
C₁₁
C₁₂
C₁₃
C₁₄
C₁₅
C₁₆
C₁₇
C₁₈
C₁₉
C₂₀
C₂₁
C₂₂
C₂₃
C₂₄

ELEMENTS

0
1, 3, 9, 27, 81
2, 6, 18, 54, 41
4, 12, 36, 108, 82
5, 15, 45, 14, 42
7, 21, 63, 68, 83
8, 24, 72, 95, 43
10, 30, 90, 28, 84
11, 33, 99, 55, 44
13, 39, 117, 109, 85
16, 48, 23, 69, 86
17, 51, 32, 96, 46
19, 57, 50, 29, 87
20, 60, 59, 56, 47
22, 66, 77, 110, 88
25, 75, 104, 70, 89
26, 78, 113, 97, 49
31, 93, 37, 111, 91
34, 102, 64, 71, 92
35, 105, 73, 98, 52
38, 114, 100, 58, 53
40, 120, 118, 112, 94
61, 62, 65, 74, 101
67, 80, 119, 115, 103
76, 107, 79, 116, 106

Period: 127
Multiplier: 2

COSET

C₀
C₁
C₂
C₃
C₄
C₅
C₆
C₇

C₈

C₉

C₁₀

ELEMENTS

0
1, 2, 4, 8, 16, 32, 64
3, 6, 12, 24, 48, 96, 65
5, 10, 20, 40, 80, 33, 66
7, 14, 28, 56, 112, 97, 67
9, 18, 36, 72, 17, 34, 68
11, 22, 44, 88, 49, 98, 69
13, 26, 52, 104, 81, 35,
70
15, 30, 60, 120, 113, 99,
71
19, 38, 76, 25, 50, 100,
73
21, 42, 84, 41, 82, 37, 74

C ₁₁	23, 46, 92, 57, 114, 101, 75
C ₁₂	27, 54, 108, 89, 51, 102, 77
C ₁₃	29, 58, 116, 105, 83, 39, 78
C ₁₄	31, 62, 124, 121, 115, 103, 79
C ₁₅	43, 86, 45, 90, 53, 106, 85
C ₁₆	47, 94, 61, 122, 117, 107, 87
C ₁₇	55, 110, 93, 59, 118, 109, 91
C ₁₈	63, 126, 125, 123, 119, 111, 95

Period: 133
Multiplier: 5

<u>COSET</u>	<u>ELEMENTS</u>
C ₀	0
C ₁	1, 5, 25, 125, 93, 66, 64, 54, 4, 20, 100, 101, 106, 131, 123, 83, 16, 80
C ₂	2, 10, 50, 117, 53, 132, 128, 108, 8, 40, 67, 69, 79, 129, 113, 33, 32, 27
C ₃	3, 15, 75, 109, 13, 65, 59 29, 12, 60, 34, 37, 52, 127, 103, 116, 48, 107
C ₄	6, 30, 17, 85, 26, 130, 118, 58, 24, 120, 68, 74, 104, 121, 73, 99, 96, 81
C ₅	7, 35, 42, 77, 119, 63, 49 112, 28
C ₆	9, 45, 92, 61, 39, 62, 44, 87, 36, 47, 102, 111, 23, 115, 43, 82, 11, 55
C ₇	14, 70, 84, 21, 105, 126, 98, 91, 56
C ₈	18, 40, 51, 122, 78, 124, 88, 41, 72, 94, 71, 89, 46, 97, 86, 31, 22, 110
C ₉	19, 95, 76, 114, 38, 57

Period: 133
Multiplier: 11

<u>COSET</u>	<u>ELEMENTS</u>
C ₀	0
C ₁	1, 11, 21
C ₂	2, 22, 109
C ₃	3, 33, 97
C ₄	4, 44, 85
C ₅	5, 55, 73
C ₆	6, 66, 61
C ₇	7, 77, 49
C ₈	8, 88, 37
C ₉	9, 99, 25
C ₁₀	10, 110, 13
C ₁₁	12, 132, 122
C ₁₂	14, 21, 98
C ₁₃	15, 32, 86
C ₁₄	16, 43, 74
C ₁₅	17, 54, 62
C ₁₆	18, 65, 50
C ₁₇	19, 76, 38
C ₁₈	20, 87, 26
C ₁₉	23, 120, 123
C ₂₀	24, 131, 111
C ₂₁	27, 31, 75
C ₂₂	28, 42, 63
C ₂₃	29, 53, 51
C ₂₄	30, 64, 39
C ₂₅	34, 108, 124
C ₂₆	35, 119, 112
C ₂₇	36, 130, 100
C ₂₈	40, 41, 52
C ₂₉	45, 96, 125
C ₃₀	46, 107, 113
C ₃₁	47, 118, 101
C ₃₂	48, 129, 89
C ₃₃	56, 84, 126
C ₃₄	57, 95, 114
C ₃₅	58, 106, 102
C ₃₆	59, 117, 90
C ₃₇	60, 128, 78
C ₃₈	67, 72, 127
C ₃₉	68, 83, 115
C ₄₀	69, 94, 103
C ₄₁	70, 105, 91
C ₄₂	71, 116, 79
C ₄₃	80, 82, 104
C ₄₄	81, 93, 92

APPENDIX C

INEQUIVALENT CROSS-CORRELATIONS

(v, k, λ)	No. of Cosets	No. of Values for $C(\tau)$
(31, 6, 1)	11	6
(31A, 15, 7)	7	
(31, 6, 1)	11	5
(31B, 15, 7)	3	
(31A, 15, 7)	7	3
(31B, 15, 7)	3	
(43A, 21, 10)	7	6
(43B, 21, 10)	3	
(63A, 31, 15)	13	4
(63B, 31, 15)	13	
(121A, 40, 13)	25	10
(121B, 40, 13)	25	
(121A, 40, 13)	25	5
(121C, 40, 13)	25	
(121A, 40, 13)	25	10
(121D, 40, 13)	25	
(121B, 40, 13)	25	9
(121C, 40, 13)	25	
(121B, 40, 13)	25	10
(121D, 40, 13)	25	
(121C, 40, 13)	25	10
(121D, 40, 13)	25	
(127A, 63, 31)	3	6
(127B, 63, 31)	19	
(127A, 63, 31)	3	5
(127C, 63, 31)	19	
(127A, 63, 31)	3	9
(127D, 63, 31)	19	

(v, k, λ)	No. of Cosets	No. of Values for $C(\tau)$
(127A, 63, 31)	3	9
(127E, 63, 31)	19	
(127A, 63, 31)	3	9
(127F, 63, 31)	19	
(127B, 63, 31)	19	3
(127C, 63, 31)	19	
(127B, 63, 31)	19	11
(127D, 63, 31)	19	
(127B, 63, 31)	19	6
(127E, 63, 31)	19	
(127B, 63, 31)	19	10
(127F, 63, 31)	19	
(127C, 63, 31)	19	10
(127D, 63, 31)	19	
(127C, 63, 31)	19	9
(127E, 63, 331)	19	
(127C, 63, 31)	19	11
(127F, 63, 31)	19	
(127D, 63, 31)	19	11
(127E, 63, 31)	19	
(127D, 63, 31)	19	11
(127F, 63, 31)	19	
(127E, 63, 31)	19	11
(127F, 63, 31)	19	
(133, 12, 1)	44	8
(133, 33, 8)	9	

APPENDIX D

EQUIVALENT CROSS-CORRELATIONS

(v, k, λ)	No. of Cosets	$\{s_{qk}\}$	$[q]$	$ C(\tau) $
$(15, 7, 3)$	5		7	4
$(21, 5, 1)$	6		5	3
$(31, 6, 1)$	11		2	3
			3	4
			4	4
			6	3
			8	4
			11	4
			12	4
			16	3
			17	4
$(31A, 15, 7)$	7		3	3
			9	3
			27	6
			19	3
			26	3
$(35, 17, 8)$	5		2	5
$(40, 13, 4)$	13		7	7
			11	6
			13	6
$(43A, 21, 10)$	7		2	6
			3	6
			6	6
			7	6
			9	6
$(57, 8, 11)$	21		2	3
			4	5
			5	5
			8	3
			10	4
			11	5
			16	5
			22	4
			23	5
			24	4

(v, k, λ)	No. of Cosets	$\{s_{qk}\}$	$[q]$	$ C(\tau) $
			29	3
			30	3
			31	4
(63A, 31, 15)	13		5	3
			11	5
			13	3
			23	5
			31	8
(63B, 31, 15)	13		5	7
			11	5
			13	7
			23	5
			31	8
(85, 21, 5)	12		3	4
			7	7
			9	4
			13	4
			21	6
			29	4
			37	7
(91, 10, 1)	17		2	3
			4	4
			5	4
			8	4
			10	3
			16	5
			19	4
			20	4
			23	4
			29	5
			46	3
(121A, 40, 13)	25		2	3
			4	3
			5	3
			7	5
			8	11
			10	3
			13	3
			16	11
			17	5
			19	5
			20	11
			25	5
			26	3
			31	3

(v, k, λ)	No. of Cosets	$\{s_{qk}\}$	$[q]$	$ C(\tau) $
			34	5
			35	5
			38	11
			40	11
			61	3
			67	11
(121A, 40, 13)	25		76	11
(121B, 40, 13)	25		2	10
			4	10
			5	10
			7	11
			8	4
			10	5
			13	5
			16	10
			17	9
			19	9
			20	10
			25	10
			26	10
			31	10
			34	10
			35	11
			38	10
			40	10
			61	10
			67	10
			76	4
(121C, 40, 13)	25		2	7
			4	3
			5	10
			7	10
			8	7
			10	7
			13	7
			16	10
			17	7
			19	7
			20	3
			25	4
			26	10
			31	3
			34	4
			35	10
			38	10
			40	9
			61	7

(v, k, λ)	No. of Cosets	$\{s_{qk}\}$	$[q]$	$ C(\tau) $
		67		3
		76		7
$(121D, 40, 13)$	25	2		9
		4		10
		5		8
		7		10
		8		10
		10		9
		13		9
		16		10
		17		11
		19		11
		20		10
		25		10
		26		8
		31		10
		34		10
		35		10
		38		10
		40		10
		61		9
		67		10
		76		10
$(127B, 63, 31)$	19	3		6
		5		7
		7		6
		9		6
		11		6
		13		6
		15		6
		21		6
		23		6
		27		7
		29		6
		31		6
		43		6
		55		6
		63		7

(v, k, λ)	No. of Cosets	$\{s_{qk}\}$	$[q]$	$ C(\tau) $
(127C, 63, 31)	19	3	3	3
		5	3	3
		7	7	7
		9	3	3
		11	3	3
		13	3	3
		15	3	3
		19	7	7
		21	7	7
		23	3	3
		27	3	3
		29	3	3
		31	7	7
		43	3	3
		47	7	7
		55	7	7
		63	11	11
(127D, 63, 31)	19	3	14	14
		5	12	12
		7	14	14
		9	13	13
		11	14	14
		13	14	14
		15	13	13
		19	14	14
		21	13	13
		23	13	13
		27	13	13
		29	14	14
		31	14	14
		43	13	13
		47	14	14
		55	14	14
		63	14	14
(127E, 63, 31)	19	3	6	6
		5	8	8
		7	8	8
		9	9	9
		11	10	10
		13	10	10
		15	9	9
		19	7	7
		21	9	9
		23	10	10
		27	9	9
		29	10	10
		31	9	9
		43	6	6

(v, k, λ)	No. of Cosets	$\{s_{qk}\}$	$[q]$	$ C(\tau) $
			47	7
			55	9
(127E, 63, 31)	19		63	10
(127F, 63, 31)	19		3	6
			5	5
			7	9
			9	7
			11	6
			13	6
			15	7
			19	5
			21	7
			23	10
			27	5
			29	10
			31	7
			43	6
			47	5
			55	9
			63	10
(133, 33, 8)	10		2	7
			3	4
			6	8
			9	8
			18	5
(133, 12, 1)	45		2	3
			3	4
			4	5
			5	5
			6	5
			8	4
			9	4
			10	4
			11	3
			13	5
			14	4
			15	4
			16	4
			18	4
			19	4
			20	5
			21	5
			23	5
			24	5
			25	5
			27	5

(v, k, λ)	No. of Cosets	$\{s_{qk}\} [q]$	$ C(\tau) $
$(133, 12, 1)$	45	28	4
		29	4
		30	5
		31	4
		32	4
		35	5
		36	5
		37	5
		38	3
		39	4
		40	5
		42	5
		43	5
		44	4

LIST OF REFERENCES

1. Baumert, Leonard D., Cyclic Difference Sets, Springer-Verlag, 1971.
2. Hall, Marshall Jr., Combinatorial Theory, Blaisdell Publishing Company, 1967.
3. McEliece, Robert J., Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987.
4. Golomb, Solomon W., and others, Digital Communications with Space Applications, Prentice-Hall, Inc., 1964.
5. Lidl, Rudolph and Neiderreiter, Harald, Finite Fields, Addison-Wesley Publishing Company, Inc., 1983.
(Encyclopedia of Mathematics and its Applications, V. 20).
6. Coxeter, H. S. M., Introduction to Geometry, John Wiley & Sons, Inc., 1961.
7. Golomb, Solomon W., "On the Classification of Balanced Binary Sequences of Period $P=2^n-1$," IEEE Transactions on Information Theory, V. IT-26, No. 6, pp. 730-732, November 1980.
8. Golomb, Solomon W., Shift Register Sequences, Aegean Park Press, 1982.
9. Sarwate, Dilip V. and Pursley, Michael B., "Cross-correlation Properties of Pseudorandom and Related Sequences," IEEE Transactions on Information Theory, V. 68, No. 5, pp. 593-619, May 1980.

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2. Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3. Department Chairman, Code 53Fs Department of Mathematics Naval Postgraduate School Monterey, California 93943-5000	3
4. Captain David L. Rogers USMC 4482 Ruggles Ct. Annandale, Virginia 22003	2

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 93948-6002

Thesis
R682 Rogers
c.1 Cross-correlation of
uniform cyclic difference
set sequences.

Thesis
R682 Rogers
c.1 Cross-correlation of
uniform cyclic difference
set sequences.

thesR682

Cross-correlation of uniform cyclic diff



3 2768 000 73499 0

DUDLEY KNOX LIBRARY